왜 AWS Verify Access를 사용한 걸까?

비싸지만 AWS Verify Access를 ~~사용할 수밖에 없었던~~ 비하인드 스토리

목차

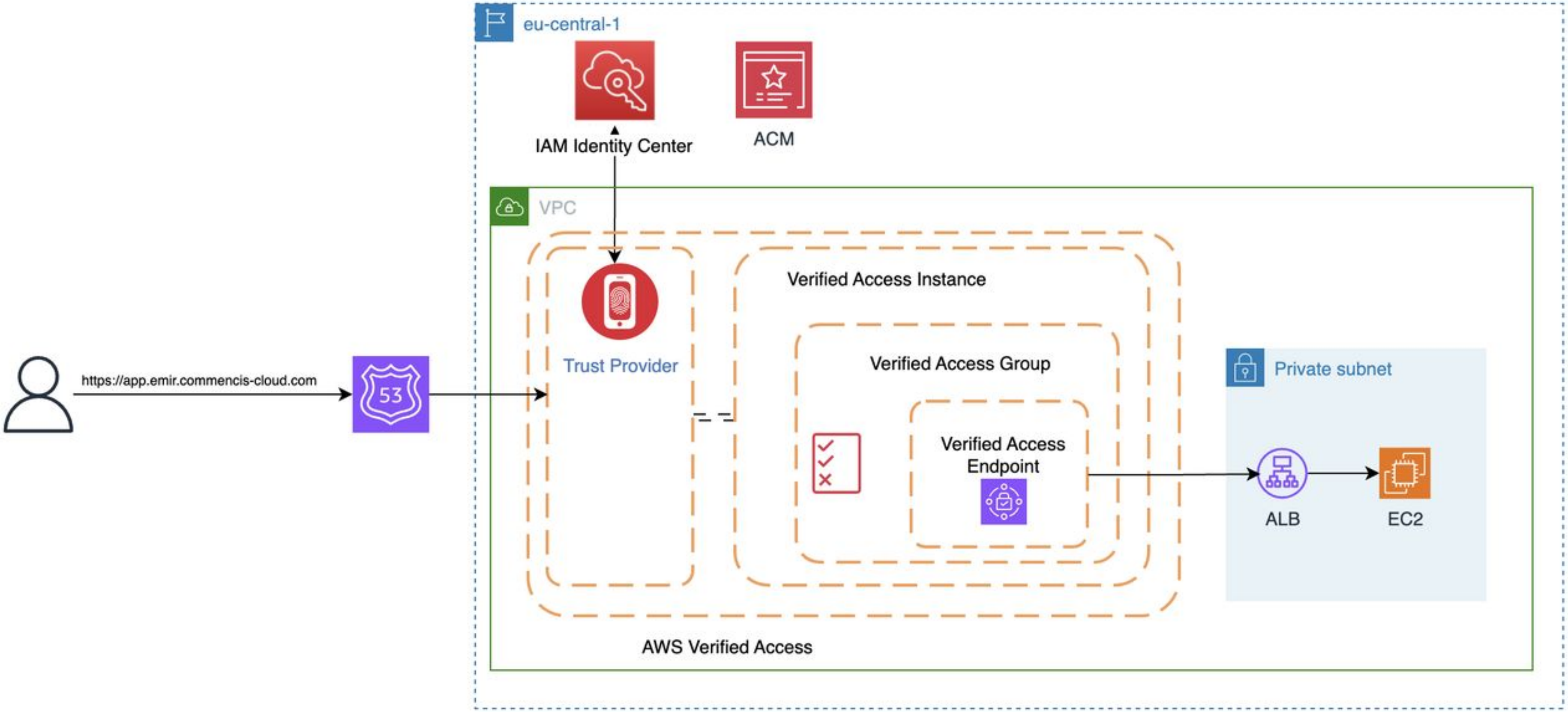
1. AVA(AWS Verify Access)이란?

2. AVA(AWS Verify Access) 이상과 현실

3. Q&A

AVA(AWS Verify Access)이란?

AVA란?


eu-central-1
IAM Identity Center
ACM
VPC
Trust Provider
Verified Access Instance
Verified Access Group
Verified Access Endpoint
Private subnet
ALB
EC2
AWS Verified Access
https://app.emir.commencis-cloud.com
53

AVA 생성 순서

(1) Verified Access trust providers (vatp)

- User / Device Trust Provider

(2) Verified Access Instances (vai)

- vatp + Logging Configuration(Optional) + AWS WAF Integrations(Optional)

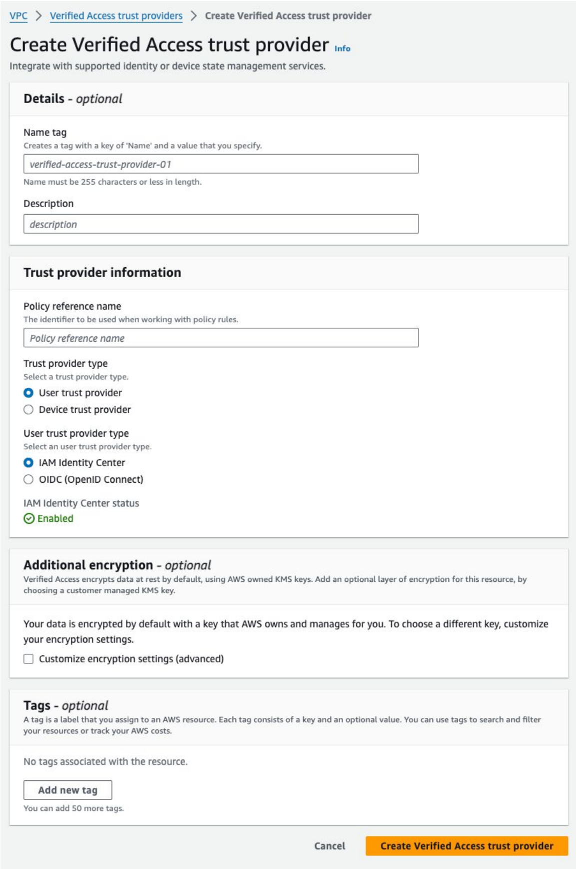
(3) Verified Access groups (vagr)

- vai + Policy(Optional)

(4) Verified Access endpoints(vae)

- vagr + Policy(Optional)

AVA란? - vatp



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

Create Verified Access trust provider Info

Integrate with supported identity or device state management services.

Details - *optional*

Name tag

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

verified-access-trust-provider-01

Name must be 255 characters or less in length.

Description

description

Trust provider information

Policy reference name

The identifier to be used when working with policy rules.

Policy reference name

Trust provider type

Select a trust provider type.

● User trust provider

○ Device trust provider

User trust provider type

Select an user trust provider type.

● IAM Identity Center

○ OIDC (OpenID Connect)

IAM Identity Center status

✓ Enabled

Additional encryption - *optional*

Verified Access encrypts data at rest by default, using AWS owned KMS keys. Add an optional layer of encryption for this resource, by choosing a customer managed KMS key.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

□ Customize encryption settings (advanced)

Tags - *optional*

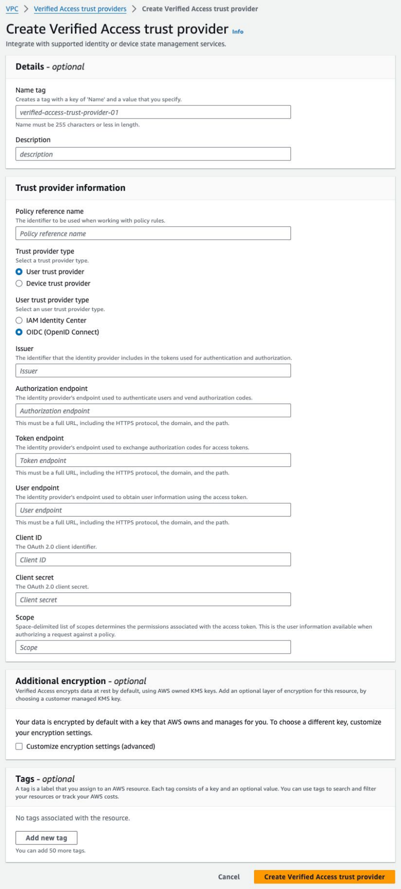
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add 50 more tags.

Cancel | Create Verified Access trust provider



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

Create Verified Access trust provider Info

Integrate with supported identity or device state management services.

Details - *optional*

Name tag

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

verified-access-trust-provider-01

Name must be 255 characters or less in length.

Description

description

Trust provider information

Policy reference name

The identifier to be used when working with policy rules.

Policy reference name

Trust provider type

Select a trust provider type.

● User trust provider

○ Device trust provider

User trust provider type

Select an user trust provider type.

○ IAM Identity Center

● OIDC (OpenID Connect)

Issuer

The identifier that the identity provider includes in the tokens used for authentication and authorization.

Issuer

Authorization endpoint

The identity provider's endpoint used to authenticate users and vend authorization codes.

Authorization endpoint

This must be a full URL, including the HTTPS protocol, the domain, and the path.

Token endpoint

The identity provider's endpoint used to exchange authorization codes for access tokens.

Token endpoint

This must be a full URL, including the HTTPS protocol, the domain, and the path.

User endpoint

The identity provider's endpoint used to obtain user information using the access token.

User endpoint

This must be a full URL, including the HTTPS protocol, the domain, and the path.

Client ID

The OAuth 2.0 client identifier.

Client ID

Client secret

The OAuth 2.0 client secret.

Client secret

Scope

Space-delimited list of scopes determines the permissions associated with the access token. This is the user information available when authorizing a request against a policy.

Scope

Additional encryption - *optional*

Verified Access encrypts data at rest by default, using AWS owned KMS keys. Add an optional layer of encryption for this resource, by choosing a customer managed KMS key.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

□ Customize encryption settings (advanced)

Tags - *optional*

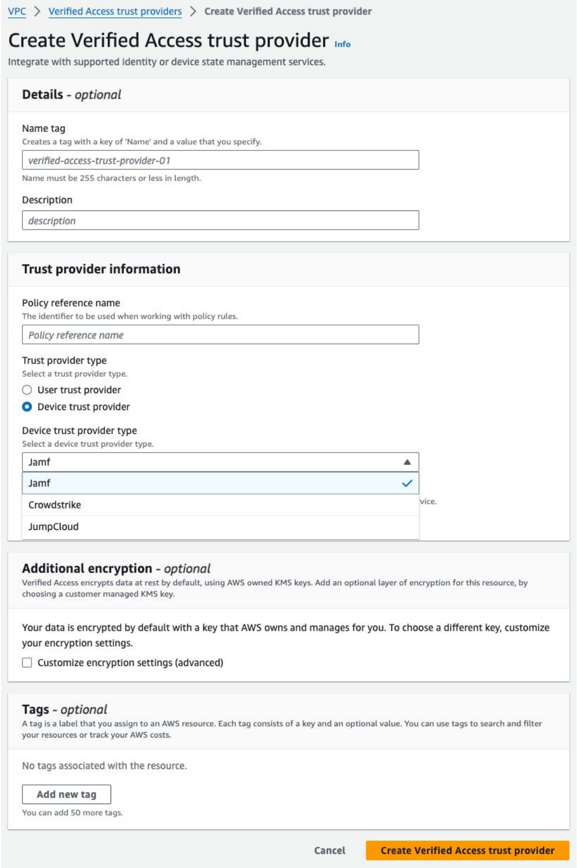
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add 50 more tags.

Cancel | Create Verified Access trust provider



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

Create Verified Access trust provider Info

Integrate with supported identity or device state management services.

Details - *optional*

Name tag

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

verified-access-trust-provider-01

Name must be 255 characters or less in length.

Description

description

Trust provider information

Policy reference name

The identifier to be used when working with policy rules.

Policy reference name

Trust provider type

Select a trust provider type.

○ User trust provider

● Device trust provider

Device trust provider type

Select a device trust provider type.

Jamf ▲

- Jamf ✓
- Crowdstrike
- JumpCloud

vice.

Additional encryption - *optional*

Verified Access encrypts data at rest by default, using AWS owned KMS keys. Add an optional layer of encryption for this resource, by choosing a customer managed KMS key.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

□ Customize encryption settings (advanced)

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.

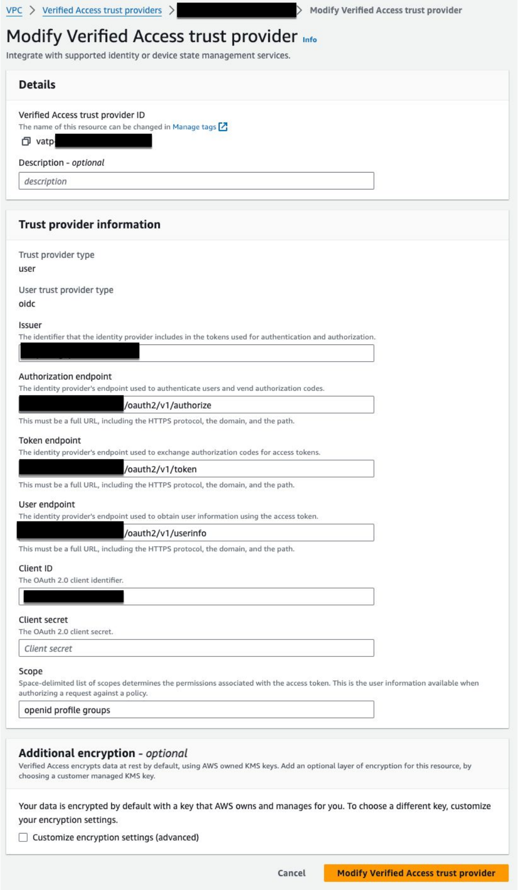
No tags associated with the resource.

Add new tag

You can add 50 more tags.

Cancel | Create Verified Access trust provider

AVA란? - vatp



VPC > Verified Access trust providers > [redacted] > Modify Verified Access trust provider

Modify Verified Access trust provider Info

Integrate with supported identity or device state management services.

Details

Verified Access trust provider ID
The name of this resource can be changed in Manage tags

vatp[redacted]

Description - *optional*

description

Trust provider information

Trust provider type
user

User trust provider type
oidc

Issuer
The identifier that the identity provider includes in the tokens used for authentication and authorization.

[redacted]

Authorization endpoint
The identity provider's endpoint used to authenticate users and vend authorization codes.

[redacted]/oauth2/v1/authorize

This must be a full URL, including the HTTPS protocol, the domain, and the path.

Token endpoint
The identity provider's endpoint used to exchange authorization codes for access tokens.

[redacted]/oauth2/v1/token

This must be a full URL, including the HTTPS protocol, the domain, and the path.

User endpoint
The identity provider's endpoint used to obtain user information using the access token.

[redacted]/oauth2/v1/userinfo

This must be a full URL, including the HTTPS protocol, the domain, and the path.

Client ID
The OAuth 2.0 client identifier.

[redacted]

Client secret
The OAuth 2.0 client secret.

Client secret

Scope
Space-delimited list of scopes determines the permissions associated with the access token. This is the user information available when authorizing a request against a policy.

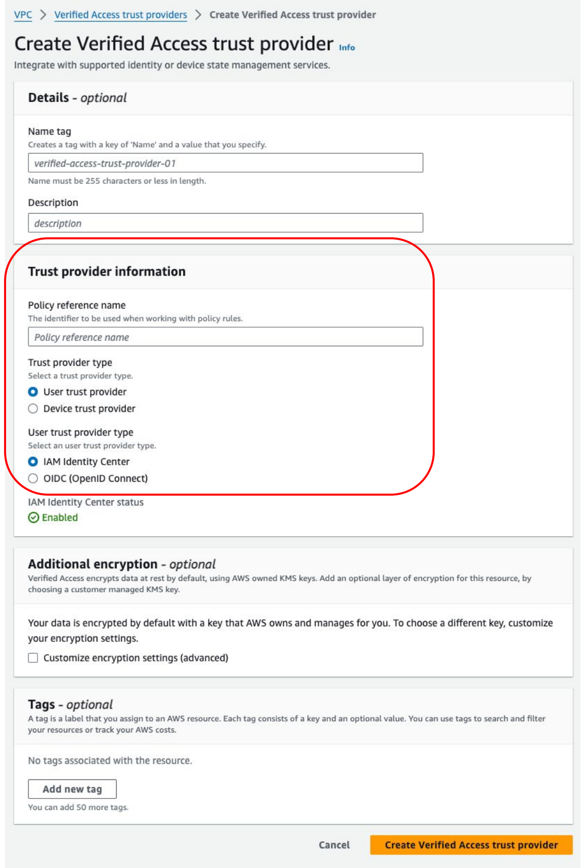
openid profile groups

Additional encryption - *optional*

Verified Access encrypts data at rest by default, using AWS owned KMS keys. Add an optional layer of encryption for this resource, by choosing a customer managed KMS key.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

□ Customize encryption settings (advanced)



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

Create Verified Access trust provider Info

Integrate with supported identity or device state management services.

Details - *optional*

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

verified-access-trust-provider-01

Name must be 255 characters or less in length.

Description

description

Trust provider information

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

Policy reference name

Trust provider type
Select a trust provider type.

● User trust provider
○ Device trust provider

User trust provider type
Select an user trust provider type.

● IAM Identity Center
○ OIDC (OpenID Connect)

IAM Identity Center status
✓ Enabled

Additional encryption - *optional*

Verified Access encrypts data at rest by default, using AWS owned KMS keys. Add an optional layer of encryption for this resource, by choosing a customer managed KMS key.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

□ Customize encryption settings (advanced)

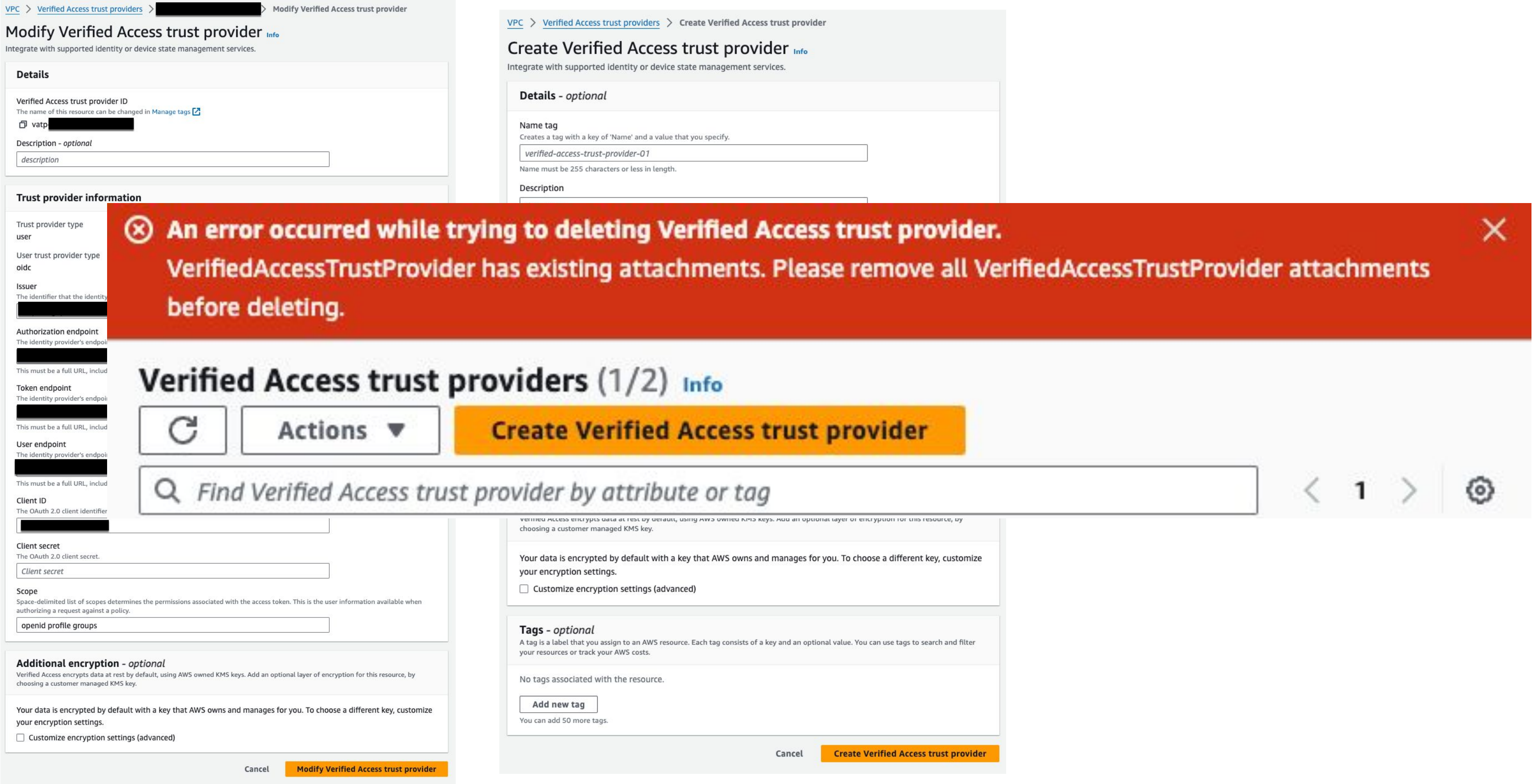
Tags - *optional*

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.

No tags associated with the resource.

You can add 50 more tags.

AVA란? - vatp



VPC > Verified Access trust providers > [redacted] > Modify Verified Access trust provider

Modify Verified Access trust provider Info

Integrate with supported identity or device state management services.

Details

Verified Access trust provider ID
The name of this resource can be changed in Manage tags
vatp[redacted]

Description - *optional*
description

Trust provider information

Trust provider type
user

User trust provider type
oidc

Issuer
The identifier that the identity
[redacted]

Authorization endpoint
The identity provider's endpoi
[redacted]
This must be a full URL, includ

Token endpoint
The identity provider's endpoi
[redacted]
This must be a full URL, includ

User endpoint
The identity provider's endpoi
[redacted]
This must be a full URL, includ

Client ID
The OAuth 2.0 client identifier
[redacted]

Client secret
The OAuth 2.0 client secret.
Client secret

Scope
Space-delimited list of scopes determines the permissions associated with the access token. This is the user information available when authorizing a request against a policy.
openid profile groups

Additional encryption - *optional*
Verified Access encrypts data at rest by default, using AWS owned KMS keys. Add an optional layer of encryption for this resource, by choosing a customer managed KMS key.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.
☐ Customize encryption settings (advanced)

Cancel | Modify Verified Access trust provider

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

Create Verified Access trust provider Info

Integrate with supported identity or device state management services.

Details - *optional*

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
verified-access-trust-provider-01
Name must be 255 characters or less in length.

Description

Verified Access encrypts data at rest by default, using AWS owned KMS keys. Add an optional layer of encryption for this resource, by choosing a customer managed KMS key.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.
☐ Customize encryption settings (advanced)

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.

No tags associated with the resource.

Add new tag
You can add 50 more tags.

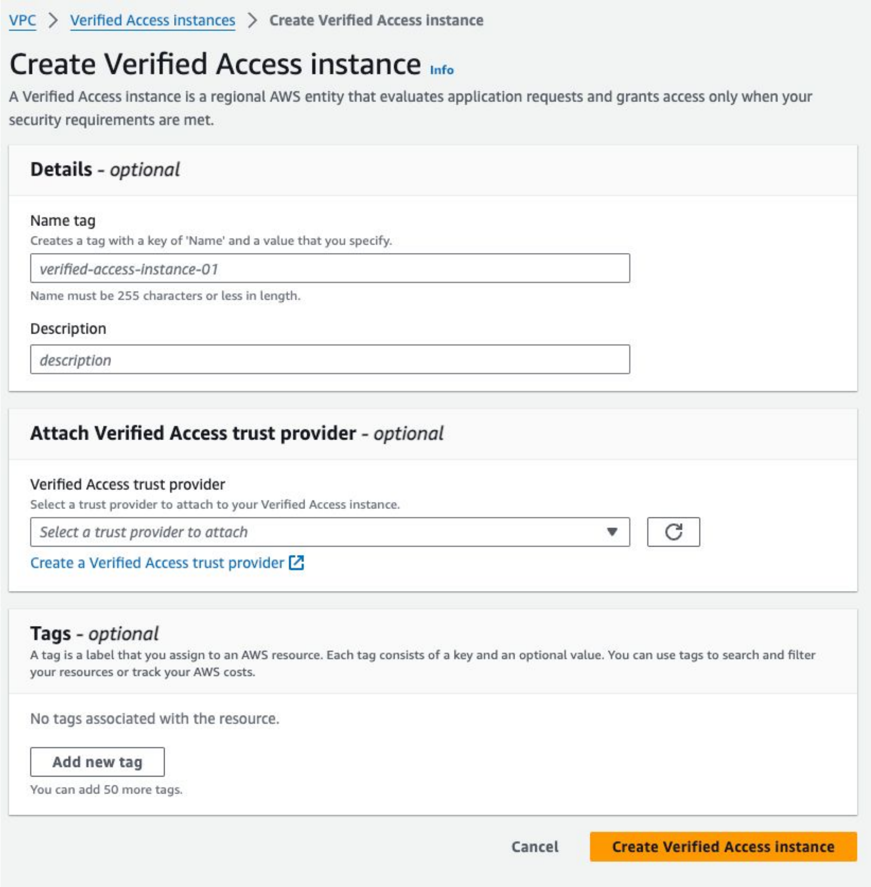
Cancel | Create Verified Access trust provider

An error occurred while trying to deleting Verified Access trust provider.
VerifiedAccessTrustProvider has existing attachments. Please remove all VerifiedAccessTrustProvider attachments before deleting.

Verified Access trust providers (1/2) Info

Actions ▼
Create Verified Access trust provider
Find Verified Access trust provider by attribute or tag
< 1 >

AVA란? - vai



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.

verified-access-instance-01

Name must be 255 characters or less in length.

Description

description

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.

No tags associated with the resource.

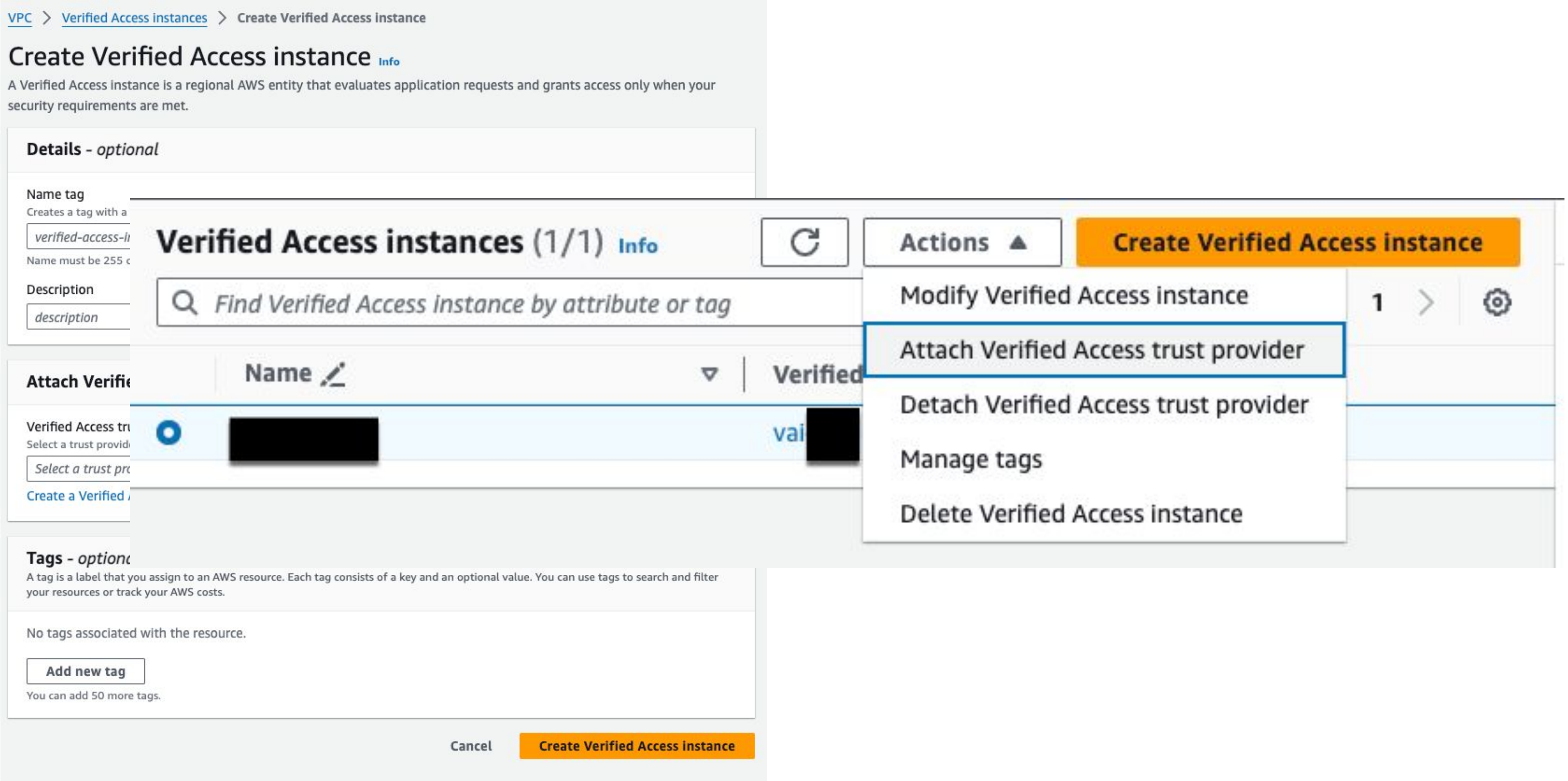
Add new tag

You can add 50 more tags.

Cancel

Create Verified Access instance

AVA란? - vai



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
verified-access-i
Name must be 255 c

Description
description

Attach Verifie

Verified Access tr
Select a trust provid
Select a trust pr
Create a Verified

Tags - *optiona*

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.

No tags associated with the resource.

Add new tag

You can add 50 more tags.

Cancel | Create Verified Access instance

Verified Access instances (1/1) Info

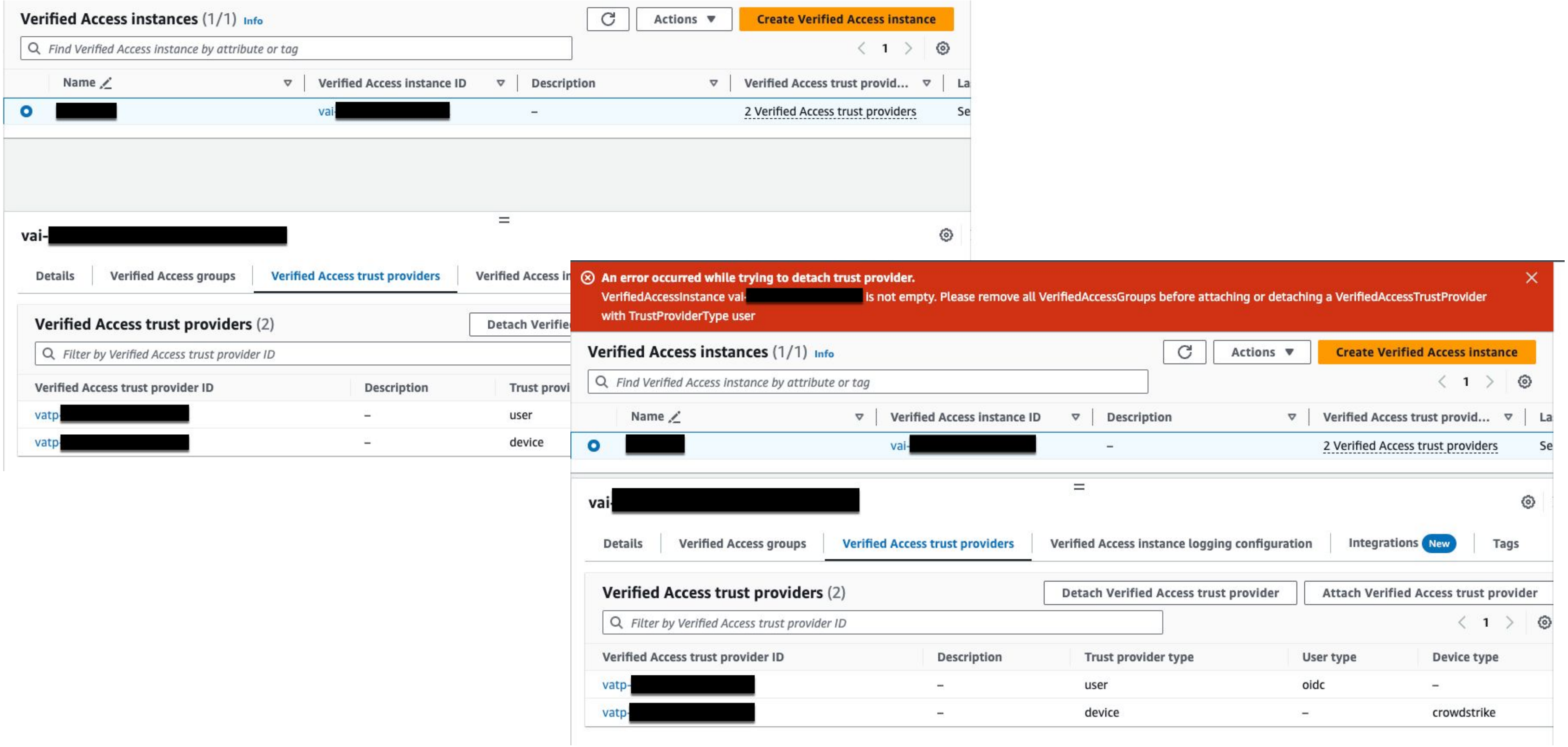
Actions ▲ | Create Verified Access instance

Find Verified Access instance by attribute or tag

- Modify Verified Access instance
- Attach Verified Access trust provider
- Detach Verified Access trust provider
- Manage tags
- Delete Verified Access instance

	Name	Verified
●	[redacted]	vai[redacted]

AVA란? - vai



Verified Access instances (1/1) Info
Actions ▼
Create Verified Access instance
Find Verified Access instance by attribute or tag
1

	Name	Verified Access instance ID	Description	Verified Access trust provid...	La
○	[redacted]	vai[redacted]	–	2 Verified Access trust providers	Se

vai-[redacted]

Details
Verified Access groups
Verified Access trust providers
Verified Access in

Verified Access trust providers (2)

Detach Verifie
Filter by Verified Access trust provider ID

Verified Access trust provider ID	Description	Trust provi
vatp[redacted]	–	user
vatp[redacted]	–	device

An error occurred while trying to detach trust provider.
VerifiedAccessInstance vai-[redacted] is not empty. Please remove all VerifiedAccessGroups before attaching or detaching a VerifiedAccessTrustProvider with TrustProviderType user

Verified Access instances (1/1) Info
Actions ▼
Create Verified Access instance
Find Verified Access instance by attribute or tag
1

	Name	Verified Access instance ID	Description	Verified Access trust provid...	La
○	[redacted]	vai-[redacted]	–	2 Verified Access trust providers	Se

vai-[redacted]

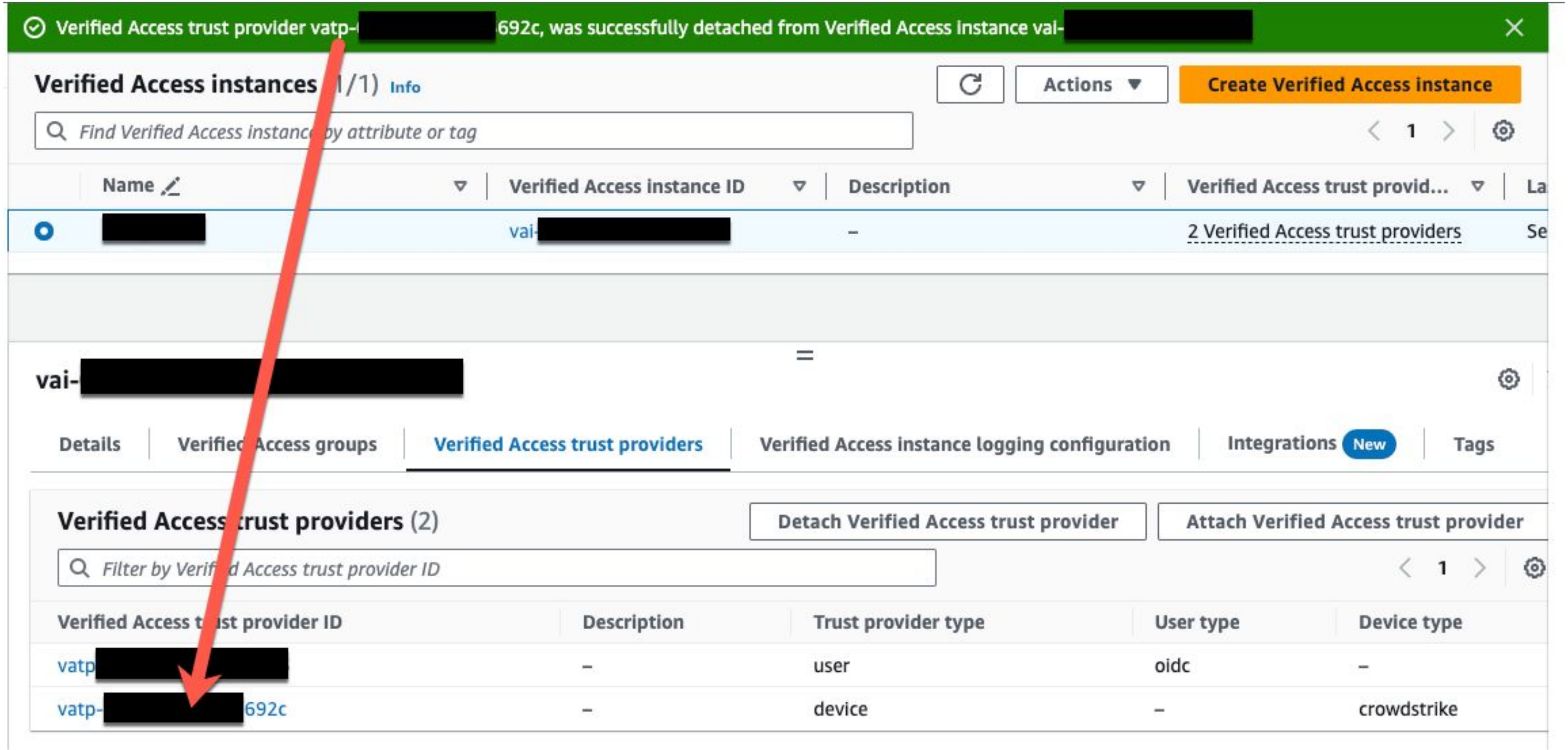
Details
Verified Access groups
Verified Access trust providers
Verified Access instance logging configuration
Integrations New
Tags

Verified Access trust providers (2)

Detach Verified Access trust provider
Attach Verified Access trust provider
Filter by Verified Access trust provider ID
1

Verified Access trust provider ID	Description	Trust provider type	User type	Device type
vatp-[redacted]	–	user	oidc	–
vatp-[redacted]	–	device	–	crowdstrike

AVA란? - vai



Verified Access trust provider vatp-[redacted]692c, was successfully detached from Verified Access instance vai-[redacted]

Verified Access instances (1/1) Info

Actions ▼
Create Verified Access instance
Find Verified Access instances by attribute or tag

	Name	Verified Access instance ID	Description	Verified Access trust provid...	La
●	[redacted]	vai-[redacted]	–	2 Verified Access trust providers	Se

vai-[redacted]

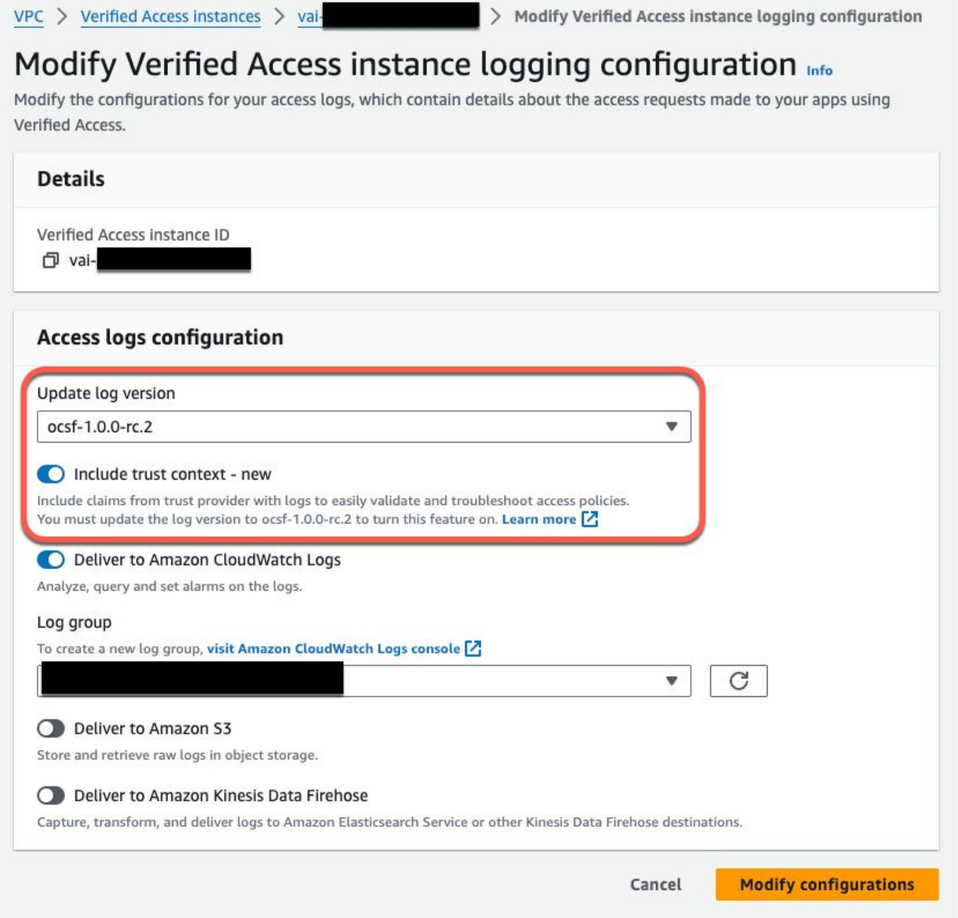
Details
Verified Access groups
Verified Access trust providers
Verified Access instance logging configuration
Integrations New
Tags

Verified Access trust providers (2)

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	Device type
vatp[redacted]	–	user	oidc	–
vatp-[redacted]692c	–	device	–	crowdstrike

AVA란? - vai



VPC > Verified Access instances > vai-[redacted] > Modify Verified Access instance logging configuration

Modify Verified Access instance logging configuration Info

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

Details

Verified Access instance ID

vai-[redacted]

Access logs configuration

Update log version

ocsf-1.0.0-rc.2 ▼

● Include trust context - new

Include claims from trust provider with logs to easily validate and troubleshoot access policies.
You must update the log version to ocsf-1.0.0-rc.2 to turn this feature on. Learn more

● 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

[redacted] ▼

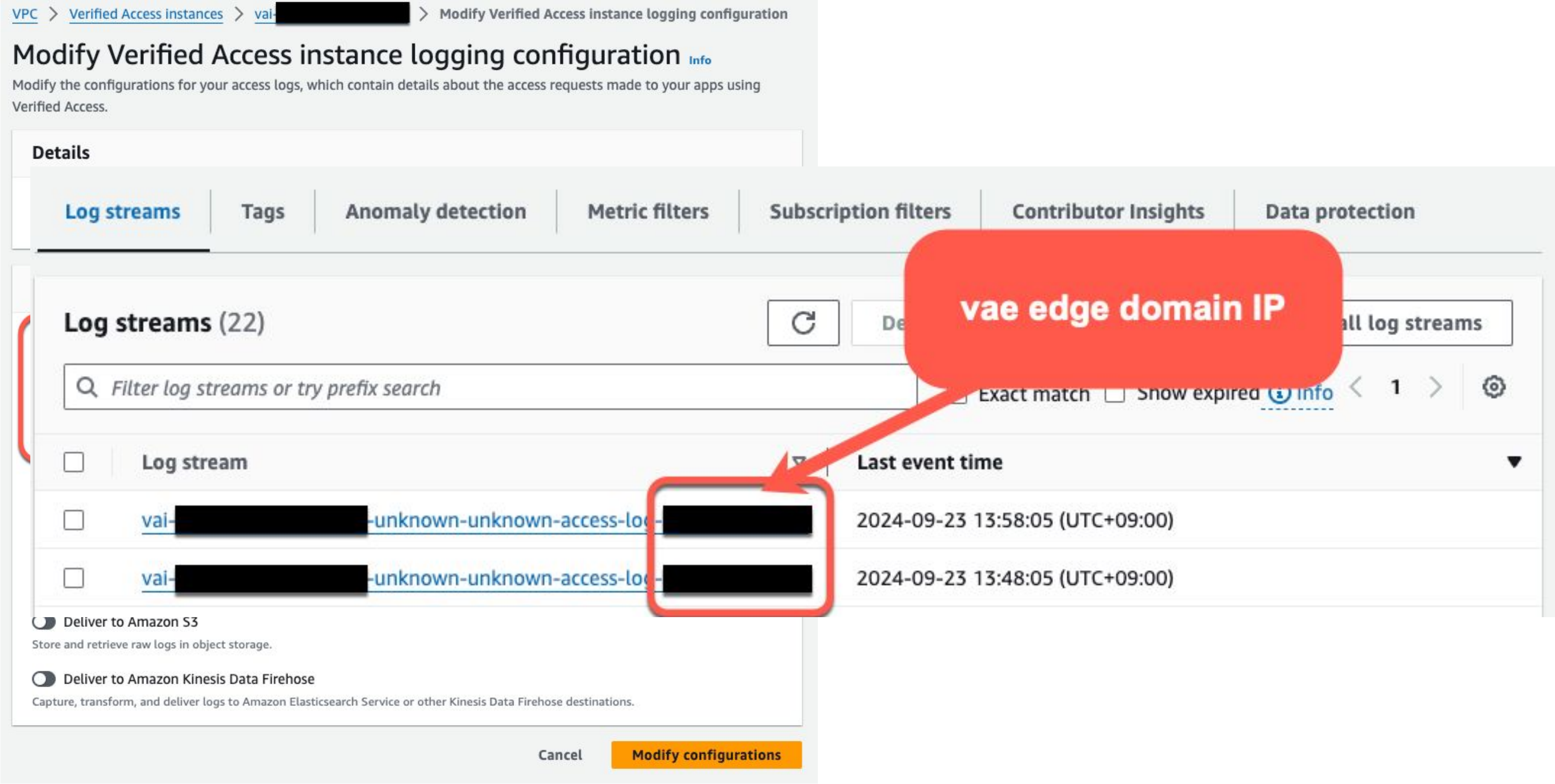
○ Deliver to Amazon S3

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.

AVA란? - vai



VPC > Verified Access instances > vai-[redacted] > Modify Verified Access instance logging configuration

Modify Verified Access instance logging configuration Info

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

Details

Log streams (22)

□	Log stream	Last event time
□	vai-[redacted]-unknown-unknown-access-lo[redacted]	2024-09-23 13:58:05 (UTC+09:00)
□	vai-[redacted]-unknown-unknown-access-lo[redacted]	2024-09-23 13:48:05 (UTC+09:00)

vae edge domain IP

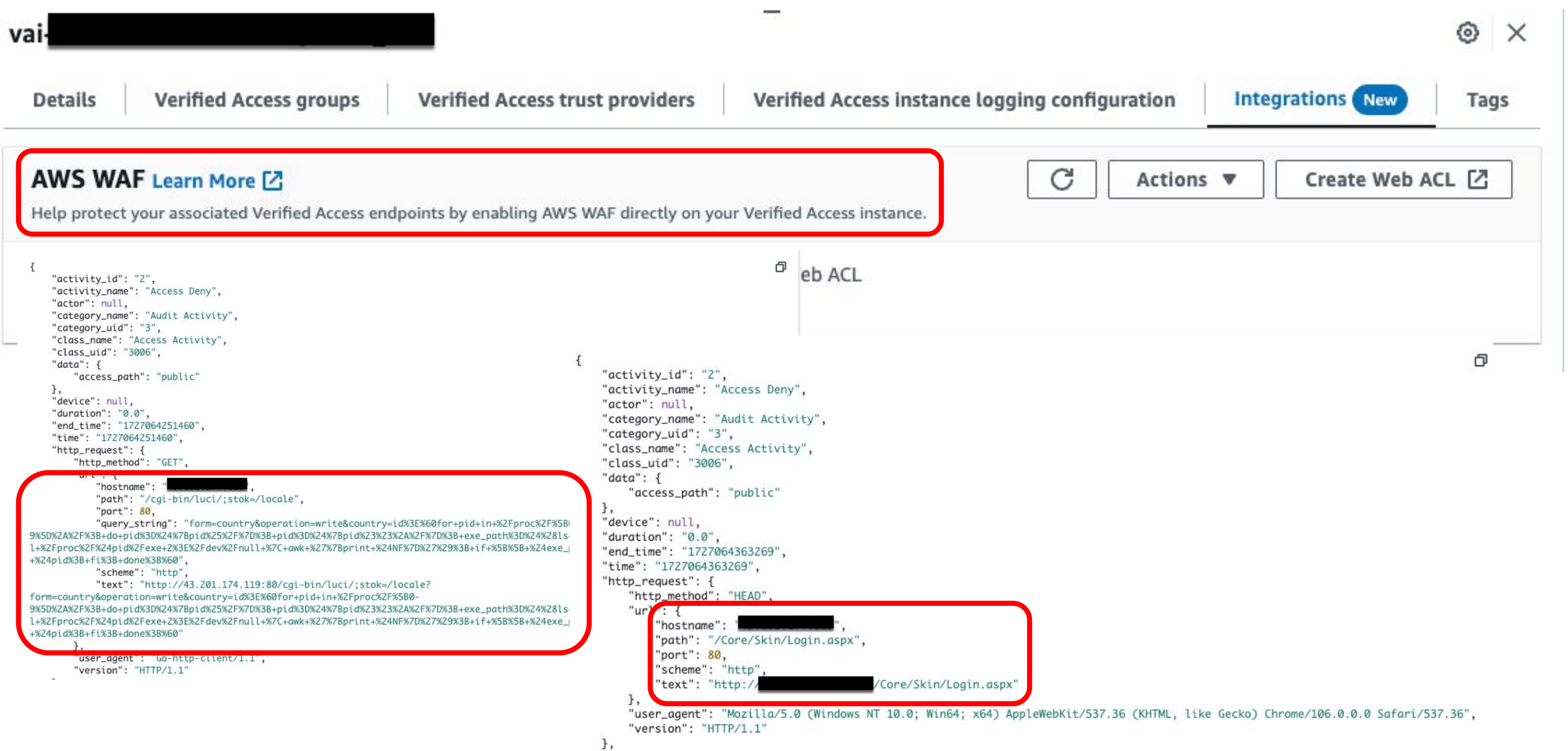
○ Deliver to Amazon S3

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.

AVA란? - vai

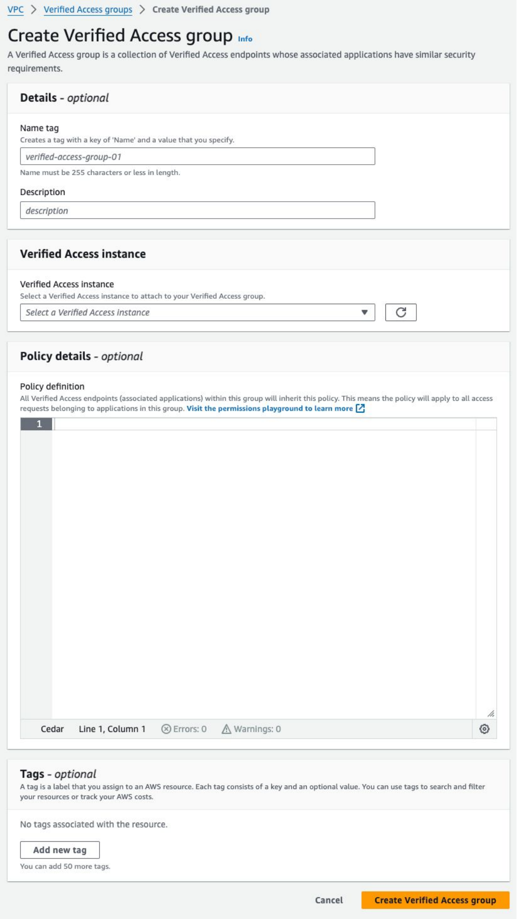


Help protect your associated Verified Access endpoints by enabling AWS WAF directly on your Verified Access instance.

```
{
    "activity_id": "2",
    "activity_name": "Access Deny",
    "actor": null,
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "data": {
        "access_path": "public"
    },
    "device": null,
    "duration": "0.0",
    "end_time": "1727064251460",
    "time": "1727064251460",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "[redacted]",
            "path": "/cgi-bin/luci/;stok=/locale",
            "port": 80,
            "query_string": "form=country&operation=write&country=id%3E%60for+pid+in+%2Fproc%2F%5B
9%5D%2A%2F%3B+do+pid%3D%24%7Bpid%25%2F%7D%3B+pid%3D%24%7Bpid%23%23%2A%2F%7D%3B+exe_path%3D%24%28ls
l+%2Fproc%2F%24pid%2Fexe+2%3E%2Fdev%2Fnull+%7C+awk+%27%7Bprint+%24NF%7D%27%29%3B+if+%5B%5B+%24exe_
+%24pid%3B+fi%3B+done%3B%60",
            "scheme": "http",
            "text": "http://43.201.174.119:80/cgi-bin/luci/;stok=/locale?
form=country&operation=write&country=id%3E%60for+pid+in+%2Fproc%2F%5B0-
9%5D%2A%2F%3B+do+pid%3D%24%7Bpid%25%2F%7D%3B+pid%3D%24%7Bpid%23%23%2A%2F%7D%3B+exe_path%3D%24%28ls
l+%2Fproc%2F%24pid%2Fexe+2%3E%2Fdev%2Fnull+%7C+awk+%27%7Bprint+%24NF%7D%27%29%3B+if+%5B%5B+%24exe_
+%24pid%3B+fi%3B+done%3B%60"
        },
        "user_agent": "Go-http-client/1.1",
        "version": "HTTP/1.1"
```

```
{
    "activity_id": "2",
    "activity_name": "Access Deny",
    "actor": null,
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "data": {
        "access_path": "public"
    },
    "device": null,
    "duration": "0.0",
    "end_time": "1727064363269",
    "time": "1727064363269",
    "http_request": {
        "http_method": "HEAD",
        "url": {
            "hostname": "[redacted]",
            "path": "/Core/Skin/Login.aspx",
            "port": 80,
            "scheme": "http",
            "text": "http:/[redacted]/Core/Skin/Login.aspx"
        },
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36",
        "version": "HTTP/1.1"
    },
```

AVA란? - vagr



VPC > Verified Access groups > Create Verified Access group

Create Verified Access group Info

A Verified Access group is a collection of Verified Access endpoints whose associated applications have similar security requirements.

Details - *optional*

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
verified-access-group-01
Name must be 255 characters or less in length.

Description
description

Verified Access instance

Verified Access instance
Select a Verified Access instance to attach to your Verified Access group.
Select a Verified Access instance ▼

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. **Visit the permissions playground to learn more**

Cedar   Line 1, Column 1   ⊗ Errors: 0   ⚠ Warnings: 0

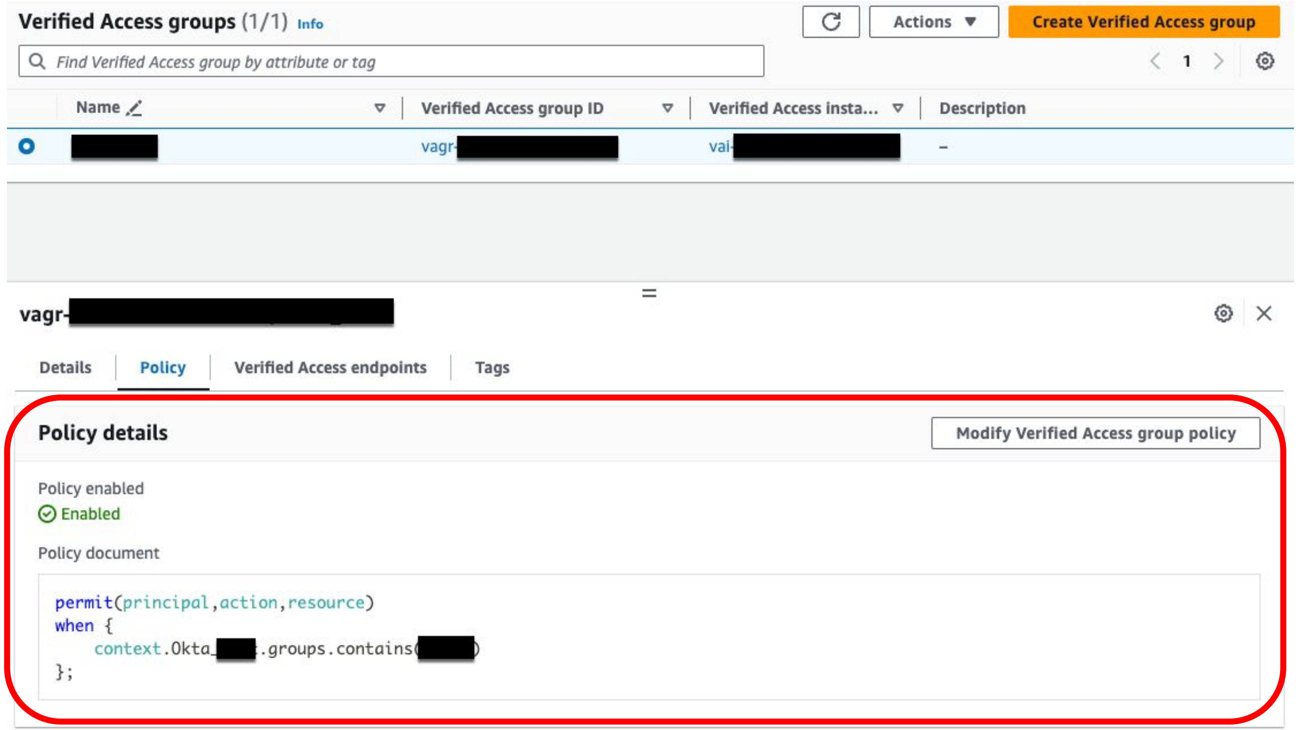
Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add 50 more tags.

Cancel   **Create Verified Access group**



Verified Access groups (1/1) Info

Actions ▼   **Create Verified Access group**

Find Verified Access group by attribute or tag   < 1 >

	Name	Verified Access group ID	Verified Access insta...	Description
●	[redacted]	vagr-[redacted]	vai-[redacted]	–

vagr-[redacted]

Details | **Policy** | Verified Access endpoints | Tags

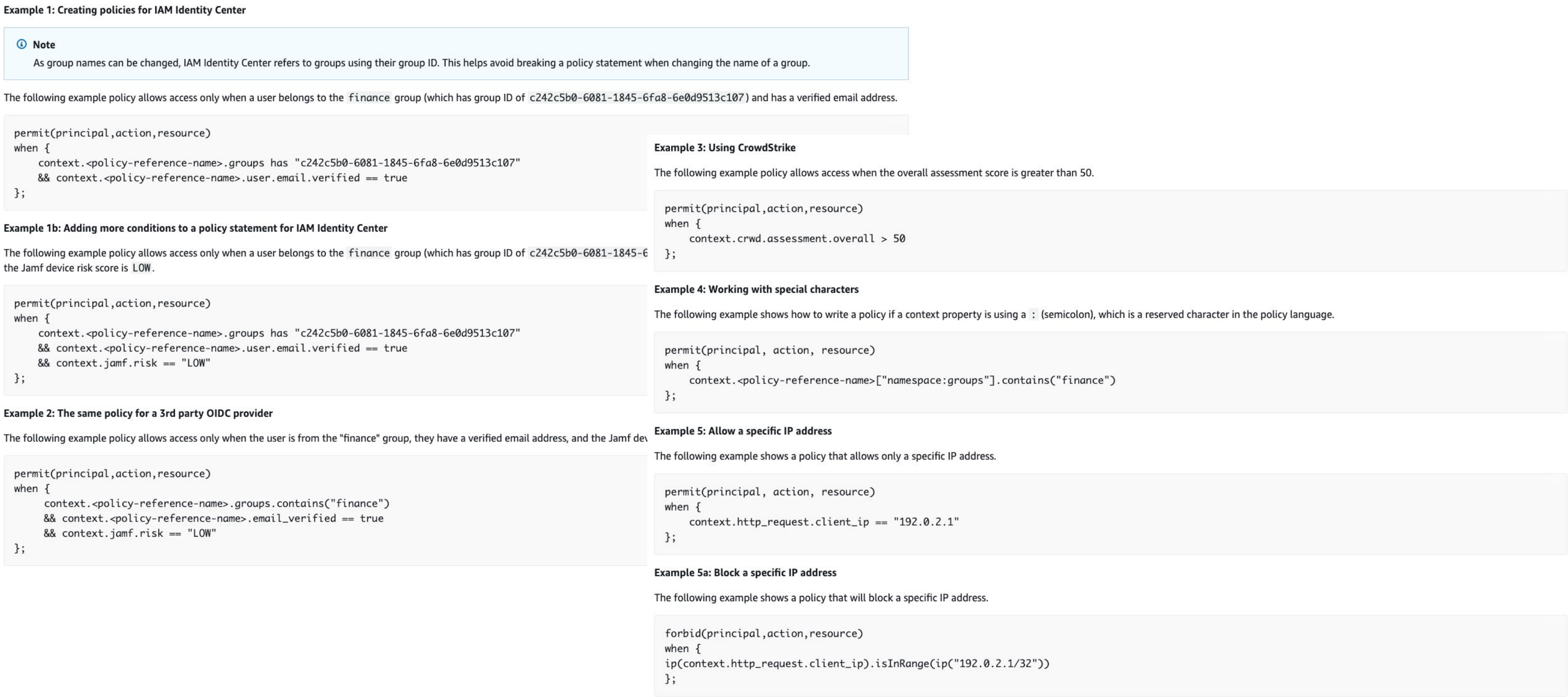
Policy details   Modify Verified Access group policy

Policy enabled
✓ Enabled

Policy document

```
permit(principal,action,resource)
when {
    context.Okta_[redacted].groups.contains([redacted])
};
```

AVA란? - vagr



Example 1: Creating policies for IAM Identity Center

ⓘ **Note**

As group names can be changed, IAM Identity Center refers to groups using their group ID. This helps avoid breaking a policy statement when changing the name of a group.

The following example policy allows access only when a user belongs to the `finance` group (which has group ID of `c242c5b0-6081-1845-6fa8-6e0d9513c107`) and has a verified email address.

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
};
```

Example 1b: Adding more conditions to a policy statement for IAM Identity Center

The following example policy allows access only when a user belongs to the `finance` group (which has group ID of `c242c5b0-6081-1845-6`
the Jamf device risk score is `LOW`.

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
    && context.jamf.risk == "LOW"
};
```

Example 2: The same policy for a 3rd party OIDC provider

The following example policy allows access only when the user is from the "finance" group, they have a verified email address, and the Jamf dev

```
permit(principal,action,resource)
when {
     context.<policy-reference-name>.groups.contains("finance")
     && context.<policy-reference-name>.email_verified == true
     && context.jamf.risk == "LOW"
};
```

Example 3: Using CrowdStrike

The following example policy allows access when the overall assessment score is greater than 50.

```
permit(principal,action,resource)
when {
    context.crwd.assessment.overall > 50
};
```

Example 4: Working with special characters

The following example shows how to write a policy if a context property is using a `:` (semicolon), which is a reserved character in the policy language.

```
permit(principal, action, resource)
when {
    context.<policy-reference-name>["namespace:groups"].contains("finance")
};
```

Example 5: Allow a specific IP address

The following example shows a policy that allows only a specific IP address.

```
permit(principal, action, resource)
when {
    context.http_request.client_ip == "192.0.2.1"
};
```

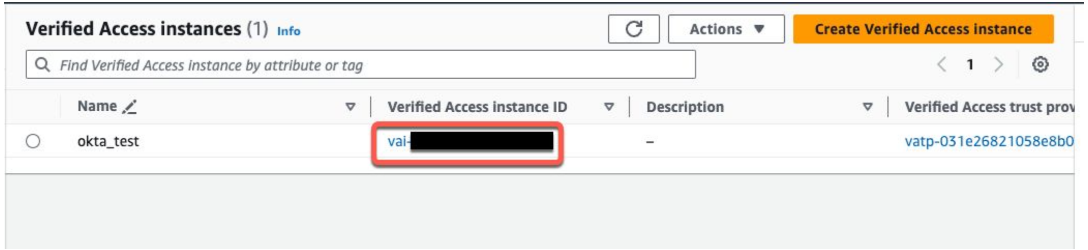
Example 5a: Block a specific IP address

The following example shows a policy that will block a specific IP address.

```
forbid(principal,action,resource)
when {
ip(context.http_request.client_ip).isInRange(ip("192.0.2.1/32"))
};
```

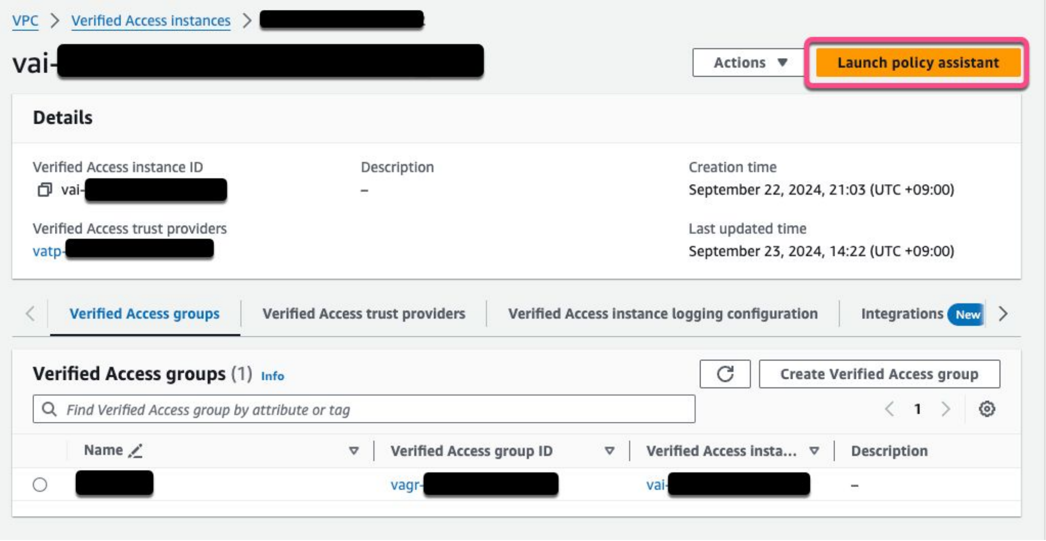
출처: Verified Access example policies

AVA란? - vagr


Actions ▼
Create Verified Access instance
Find Verified Access instance by attribute or tag
1

Verified Access instances (1) Info

	Name	Verified Access instance ID	Description	Verified Access trust prov
○	okta_test	vai-[redacted]	–	vatp-031e26821058e8b0


Actions ▼
Launch policy assistant
Create Verified Access group
Find Verified Access group by attribute or tag
1

VPC > Verified Access instances > [redacted]

vai-[redacted]

Details

Verified Access instance ID
vai-[redacted]

Description
–

Creation time
September 22, 2024, 21:03 (UTC +09:00)

Verified Access trust providers
vatp-[redacted]

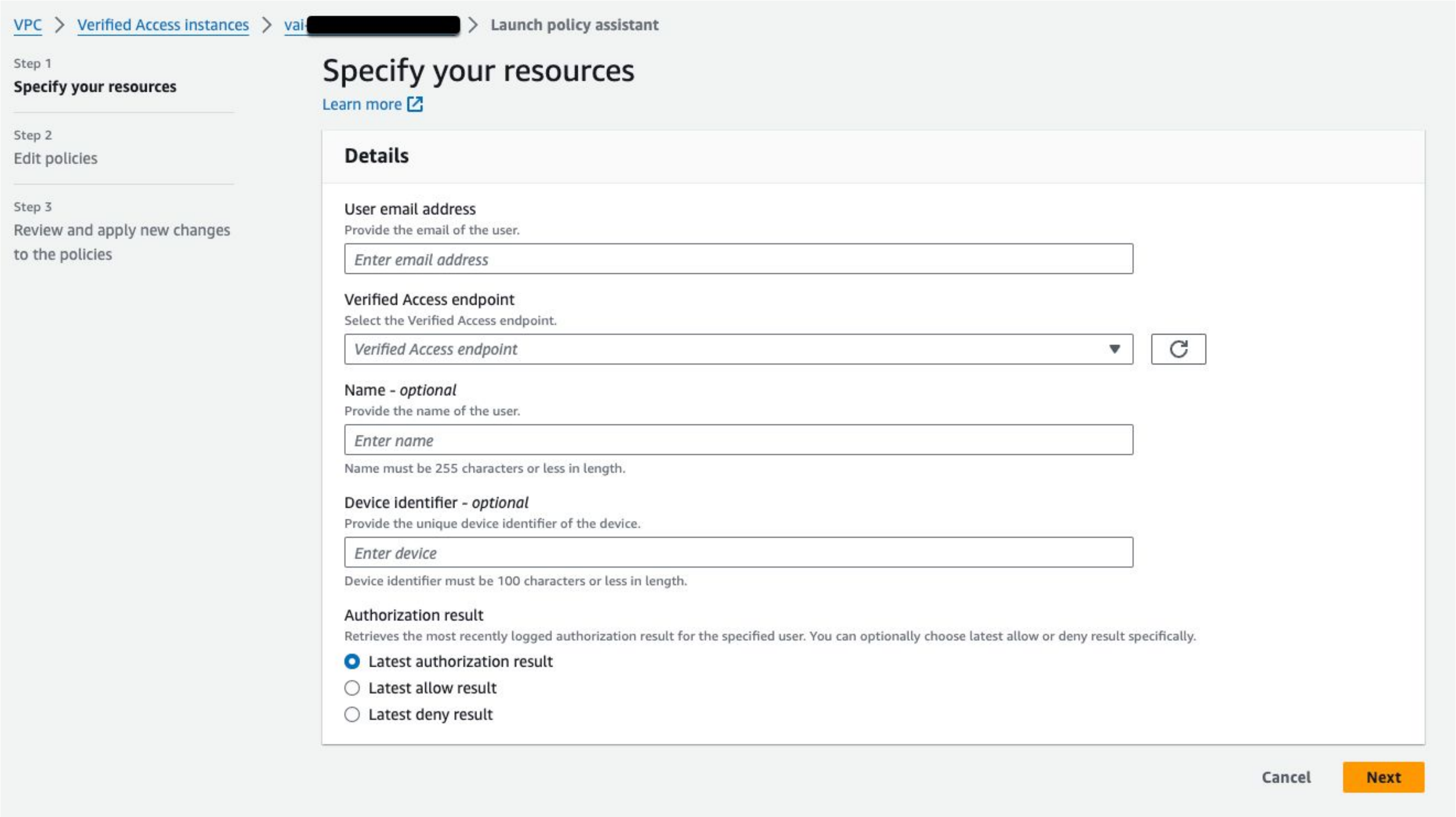
Last updated time
September 23, 2024, 14:22 (UTC +09:00)

Verified Access groups | Verified Access trust providers | Verified Access instance logging configuration | Integrations New

Verified Access groups (1) Info

	Name	Verified Access group ID	Verified Access insta...	Description
○	[redacted]	vagr-[redacted]	vai-[redacted]	–

AVA란? - vagr



VPC > Verified Access instances > vai-[redacted] > Launch policy assistant

Step 1

Specify your resources

Step 2

Edit policies

Step 3

Review and apply new changes to the policies

Specify your resources

Learn more

Details

User email address

Provide the email of the user.

Enter email address

Verified Access endpoint

Select the Verified Access endpoint.

Verified Access endpoint ▼

Name - *optional*

Provide the name of the user.

Enter name

Name must be 255 characters or less in length.

Device identifier - *optional*

Provide the unique device identifier of the device.

Enter device

Device identifier must be 100 characters or less in length.

Authorization result

Retrieves the most recently logged authorization result for the specified user. You can optionally choose latest allow or deny result specifically.

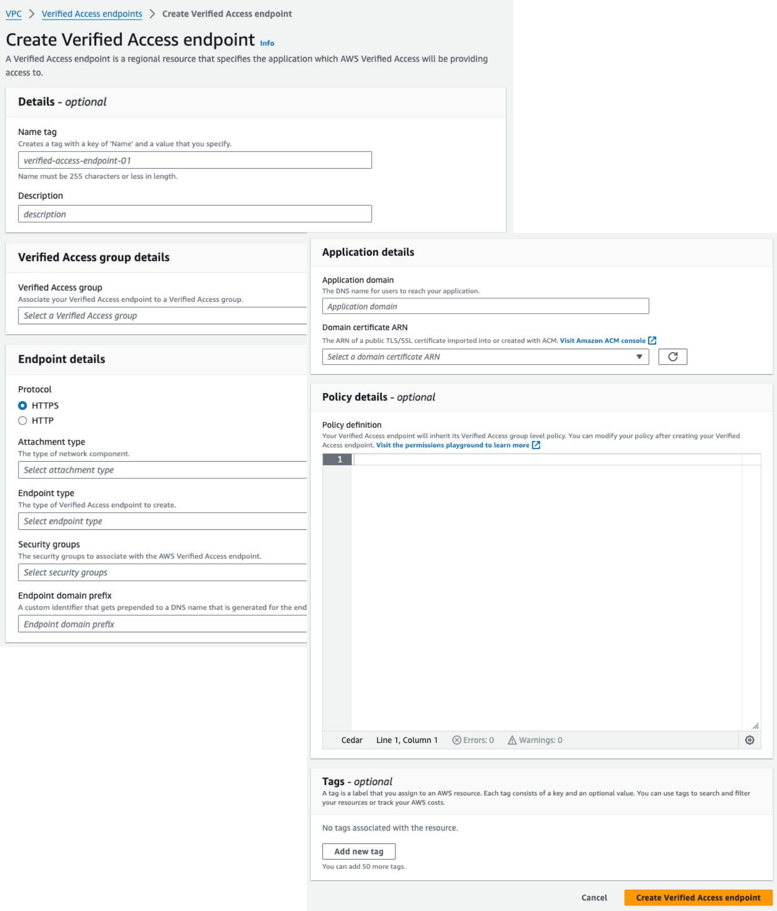
● Latest authorization result

○ Latest allow result

○ Latest deny result

출처 : Verified Access policy assistant

AVA란? - vae



VPC > Verified Access endpoints > Create Verified Access endpoint

Create Verified Access endpoint Info

A 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.
verified-access-endpoint-01
Name must be 255 characters or less in length.

Description
description

Verified Access group details

Verified Access group
Associate your Verified Access endpoint to a Verified Access group.
Select a Verified Access group

Endpoint details

Protocol
● HTTPS
○ HTTP

Attachment type
The type of network component.
Select attachment type

Endpoint type
The type of Verified Access endpoint to create.
Select endpoint type

Security groups
The security groups to associate with the AWS Verified Access endpoint.
Select security groups

Endpoint domain prefix
A custom identifier that gets prepended to a DNS name that is generated for the end
Endpoint domain prefix

Application details

Application domain
The DNS name for users to reach your application.
Application domain

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

Policy details - *optional*

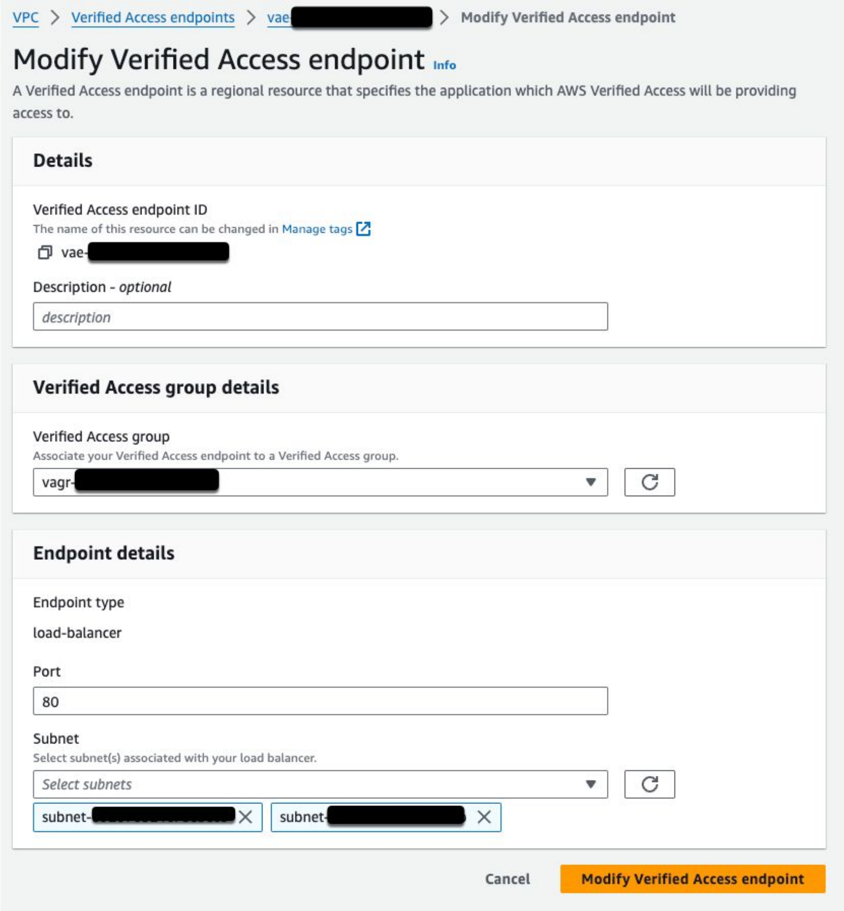
Policy definition
Your Verified Access endpoint will inherit its Verified Access group level policy. You can modify your policy after creating your Verified Access endpoint. Visit the permissions playground to learn more

Cedar 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.

No tags associated with the resource.

You can add 50 more tags.



VPC > Verified Access endpoints > vae[redacted] > Modify Verified Access endpoint

Modify Verified Access endpoint Info

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

Details

Verified Access endpoint ID
The name of this resource can be changed in Manage tags
vae-[redacted]

Description - *optional*
description

Verified Access group details

Verified Access group
Associate your Verified Access endpoint to a Verified Access group.
vagr-[redacted]

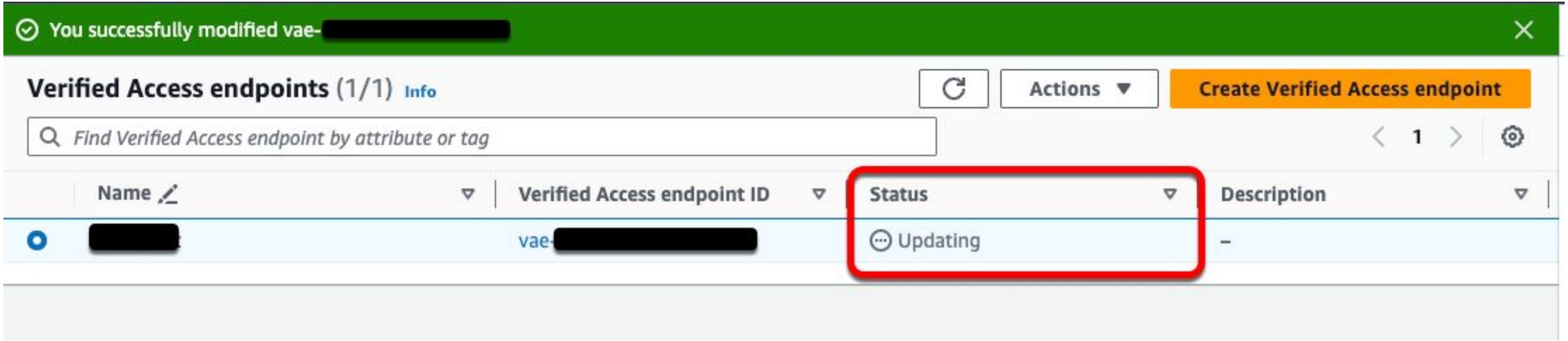
Endpoint details

Endpoint type
load-balancer

Port
80

Subnet
Select subnet(s) associated with your load balancer.
Select subnets
subnet-[redacted] ✕ subnet-[redacted] ✕

AVA란? - vae

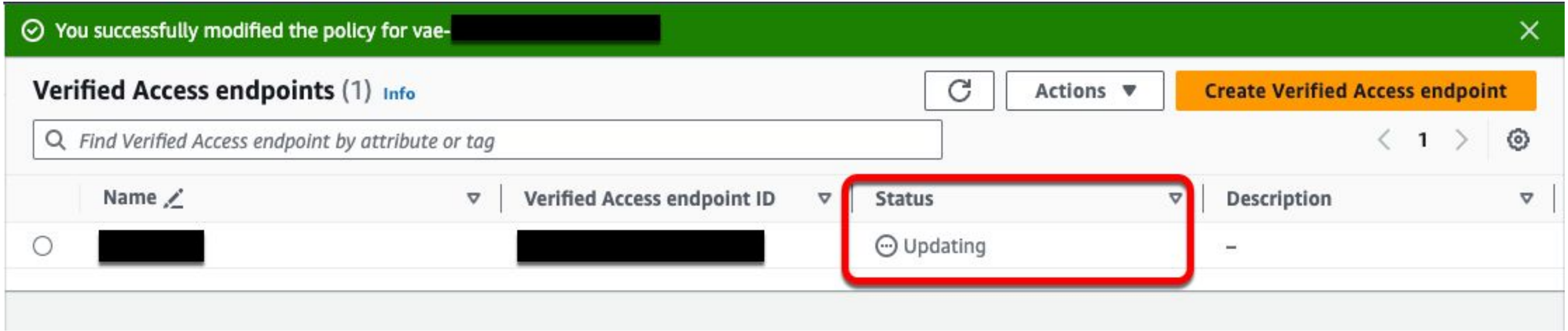


You successfully modified vae-[redacted]

Verified Access endpoints (1/1) Info

Actions ▼
Create Verified Access endpoint
Find Verified Access endpoint by attribute or tag
1

	Name	Verified Access endpoint ID	Status	Description
●	[redacted]	vae-[redacted]	Updating	–



You successfully modified the policy for vae-[redacted]

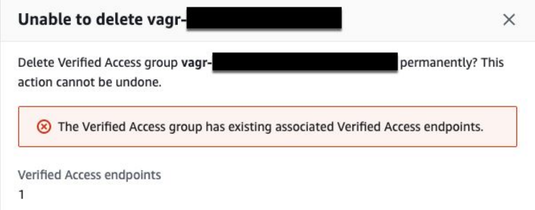
Verified Access endpoints (1) Info

Actions ▼
Create Verified Access endpoint
Find Verified Access endpoint by attribute or tag
1

	Name	Verified Access endpoint ID	Status	Description
○	[redacted]	[redacted]	Updating	–

AVA 삭제 순서

(1) Verified Access endpoints(vae)



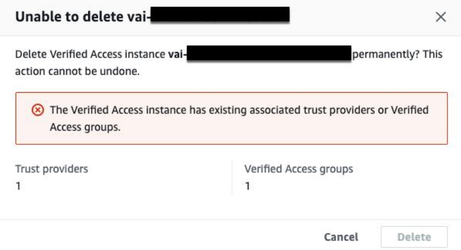
Unable to delete vagr-[redacted]

Delete Verified Access group **vagr-**[redacted] permanently? This action cannot be undone.

ⓧ The Verified Access group has existing associated Verified Access endpoints.

Verified Access endpoints
1

(2) Verified Access groups (vagr)



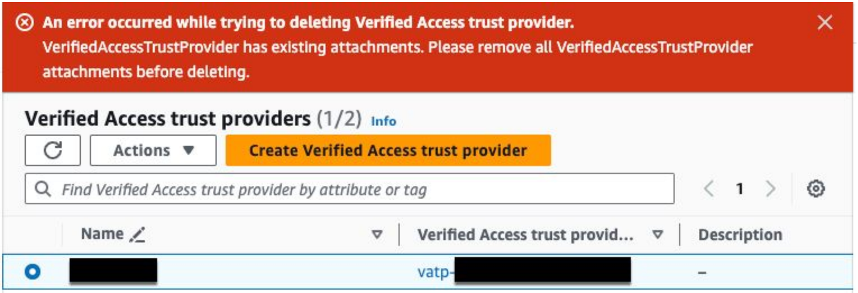
Unable to delete vai-[redacted]

Delete Verified Access instance **vai-**[redacted] permanently? This action cannot be undone.

ⓧ The Verified Access instance has existing associated trust providers or Verified Access groups.

Trust providers	Verified Access groups
1	1

(3) Verified Access Instances (vai)
 - Detach Verified Access trust provider로 vatp 연결 해제



ⓧ **An error occurred while trying to deleting Verified Access trust provider.**
VerifiedAccessTrustProvider has existing attachments. Please remove all VerifiedAccessTrustProvider attachments before deleting.

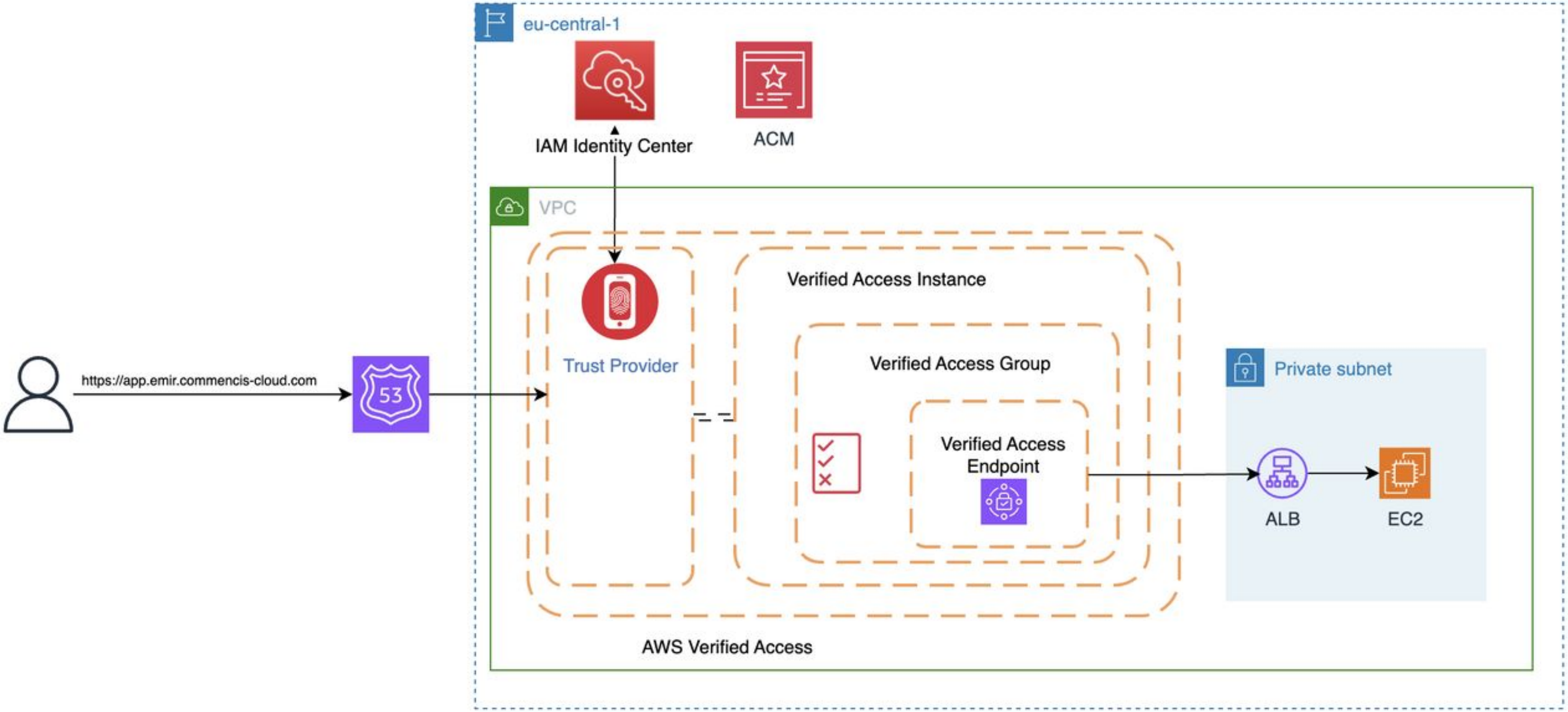
Verified Access trust providers (1/2) Info

Actions ▼
Create Verified Access trust provider
Find Verified Access trust provider by attribute or tag
1

	Name	Verified Access trust provid...	Description
●	[redacted]	vatp-[redacted]	–

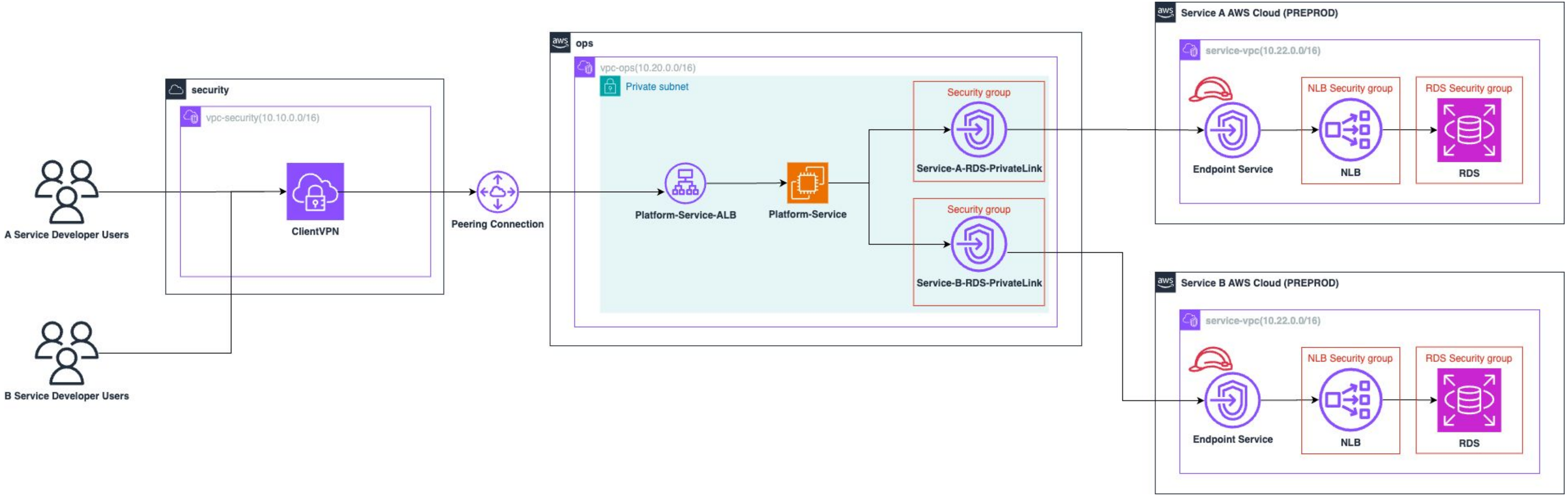
(4) Verified Access trust providers (vatp) - Option

AVA란?

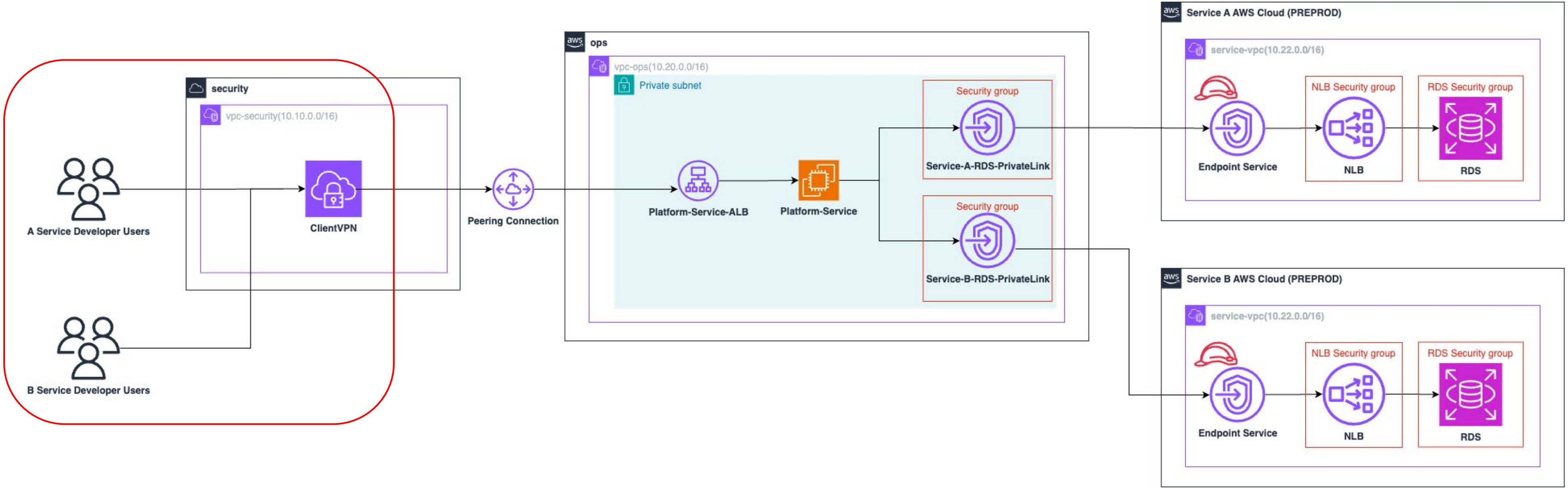

https://app.emir.commencis-cloud.com
53
eu-central-1
IAM Identity Center
ACM
VPC
Trust Provider
Verified Access Instance
Verified Access Group
Verified Access Endpoint
Private subnet
ALB
EC2
AWS Verified Access

AVA(AWS Verify Access) 이상과 현실

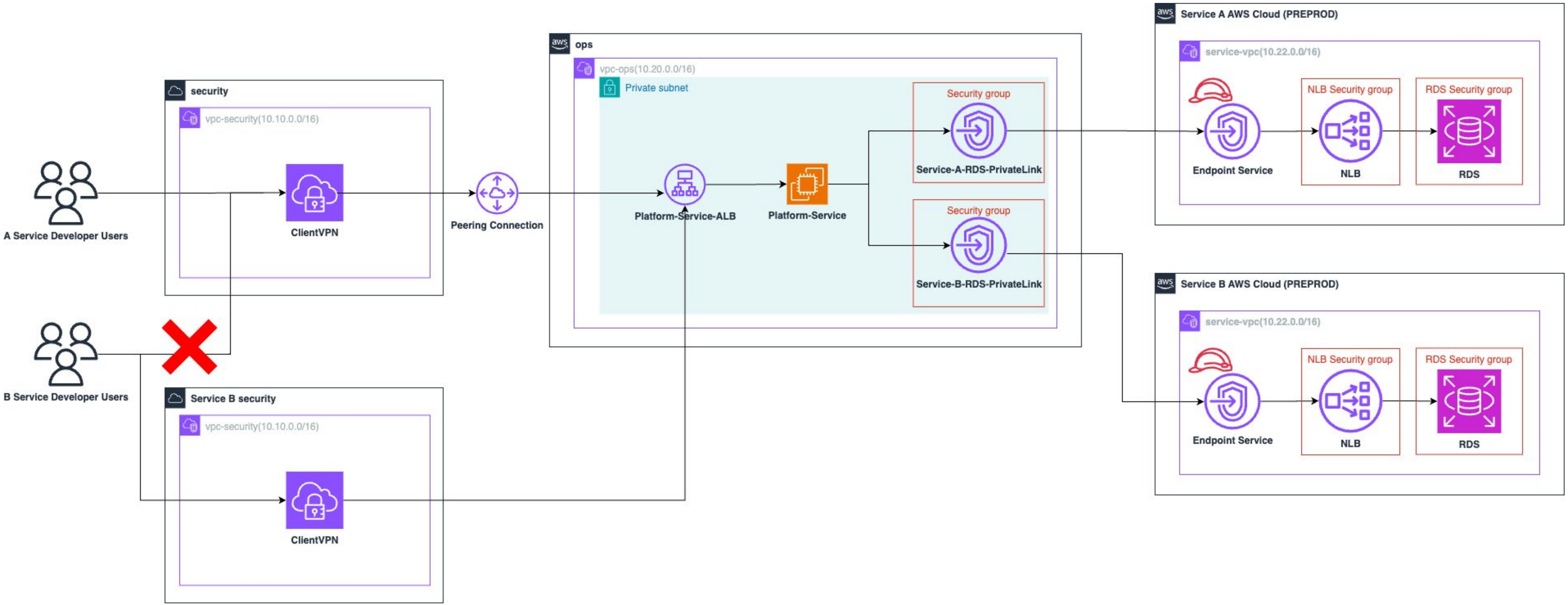
AS-IS


A Service Developer Users
B Service Developer Users
security
vpc-security(10.10.0.0/16)
ClientVPN
Peering Connection
ops
vpc-ops(10.20.0.0/16)
Private subnet
Platform-Service-ALB
Platform-Service
Security group
Service-A-RDS-PrivateLink
Security group
Service-B-RDS-PrivateLink
Service A AWS Cloud (PREPROD)
service-vpc(10.22.0.0/16)
Endpoint Service
NLB Security group
NLB
RDS Security group
RDS
Service B AWS Cloud (PREPROD)
service-vpc(10.22.0.0/16)
Endpoint Service
NLB Security group
NLB
RDS Security group
RDS

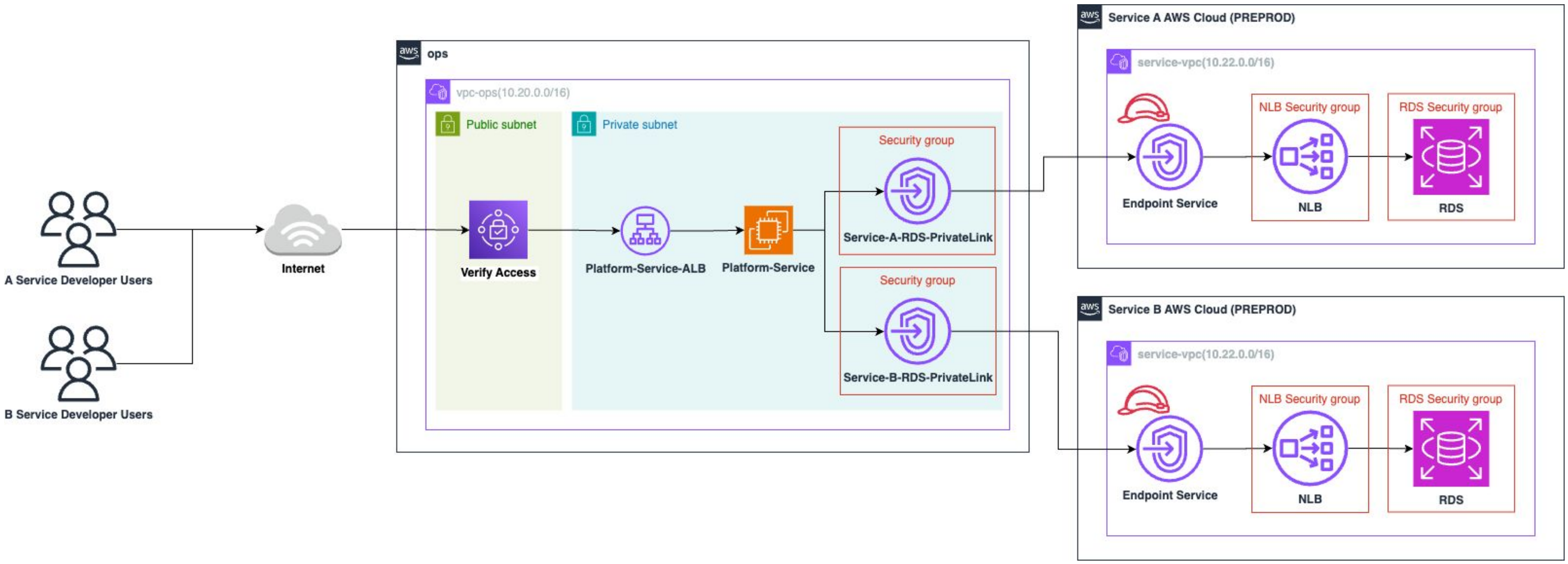
AS-IS


security
vpc-security(10.10.0.0/16)
A Service Developer Users
ClientVPN
B Service Developer Users
Peering Connection
ops
vpc-ops(10.20.0.0/16)
Private subnet
Platform-Service-ALB
Platform-Service
Security group
Service-A-RDS-PrivateLink
Security group
Service-B-RDS-PrivateLink
Service A AWS Cloud (PREPROD)
service-vpc(10.22.0.0/16)
NLB Security group
RDS Security group
Endpoint Service
NLB
RDS
Service B AWS Cloud (PREPROD)
service-vpc(10.22.0.0/16)
NLB Security group
RDS Security group
Endpoint Service
NLB
RDS

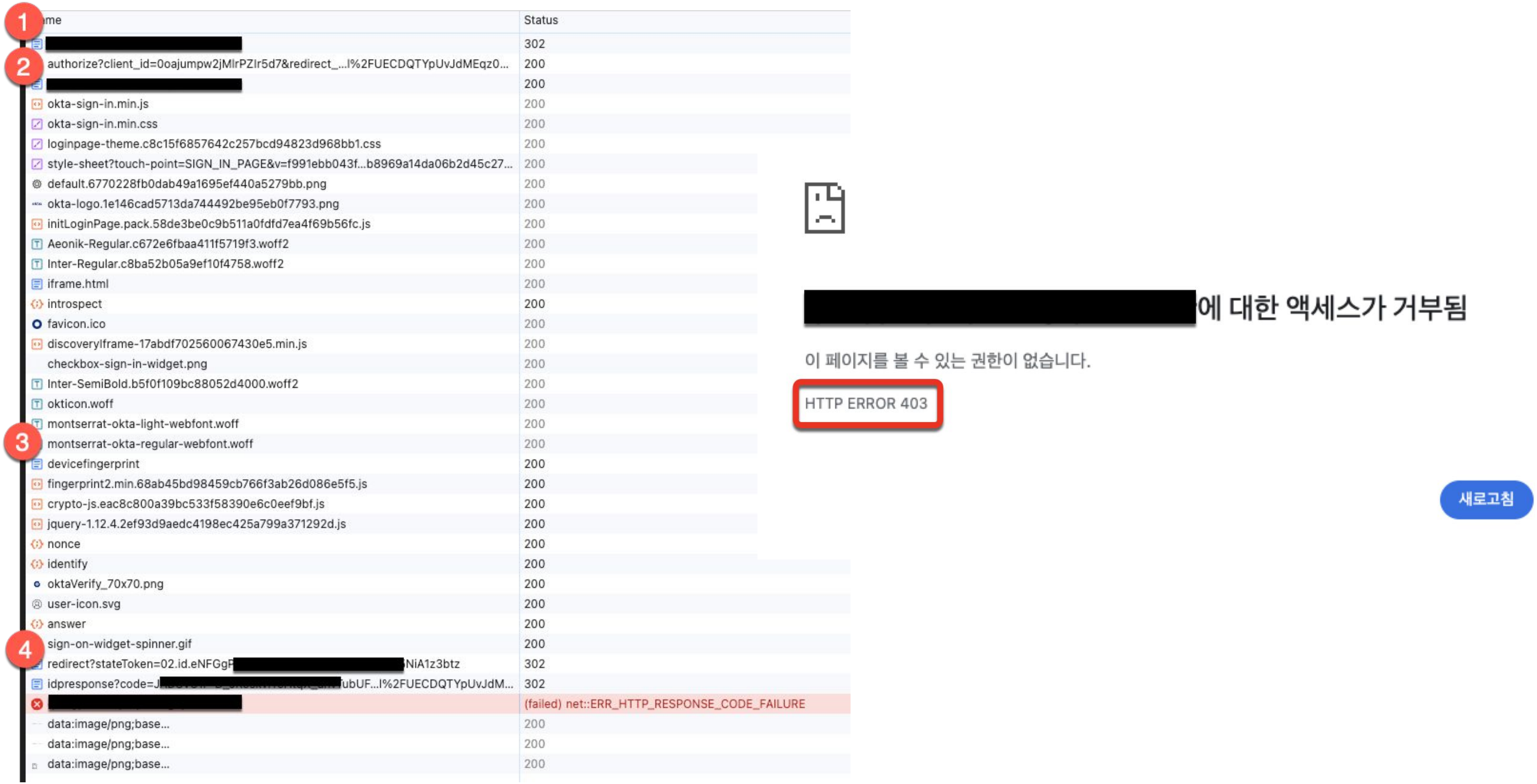
AS-IS


A Service Developer Users
B Service Developer Users
security
vpc-security(10.10.0.0/16)
ClientVPN
Service B security
vpc-security(10.10.0.0/16)
ClientVPN
Peering Connection
ops
vpc-ops(10.20.0.0/16)
Private subnet
Platform-Service-ALB
Platform-Service
Security group
Service-A-RDS-PrivateLink
Security group
Service-B-RDS-PrivateLink
Service A AWS Cloud (PREPROD)
service-vpc(10.22.0.0/16)
Endpoint Service
NLB Security group
NLB
RDS Security group
RDS
Service B AWS Cloud (PREPROD)
service-vpc(10.22.0.0/16)
Endpoint Service
NLB Security group
NLB
RDS Security group
RDS

TO-BE


A Service Developer Users
B Service Developer Users
Internet
ops
vpc-ops(10.20.0.0/16)
Public subnet
Private subnet
Verify Access
Platform-Service-ALB
Platform-Service
Security group
Service-A-RDS-PrivateLink
Security group
Service-B-RDS-PrivateLink
Service A AWS Cloud (PREPROD)
service-vpc(10.22.0.0/16)
NLB Security group
RDS Security group
Endpoint Service
NLB
RDS
Service B AWS Cloud (PREPROD)
service-vpc(10.22.0.0/16)
NLB Security group
RDS Security group
Endpoint Service
NLB
RDS

Troubleshooting



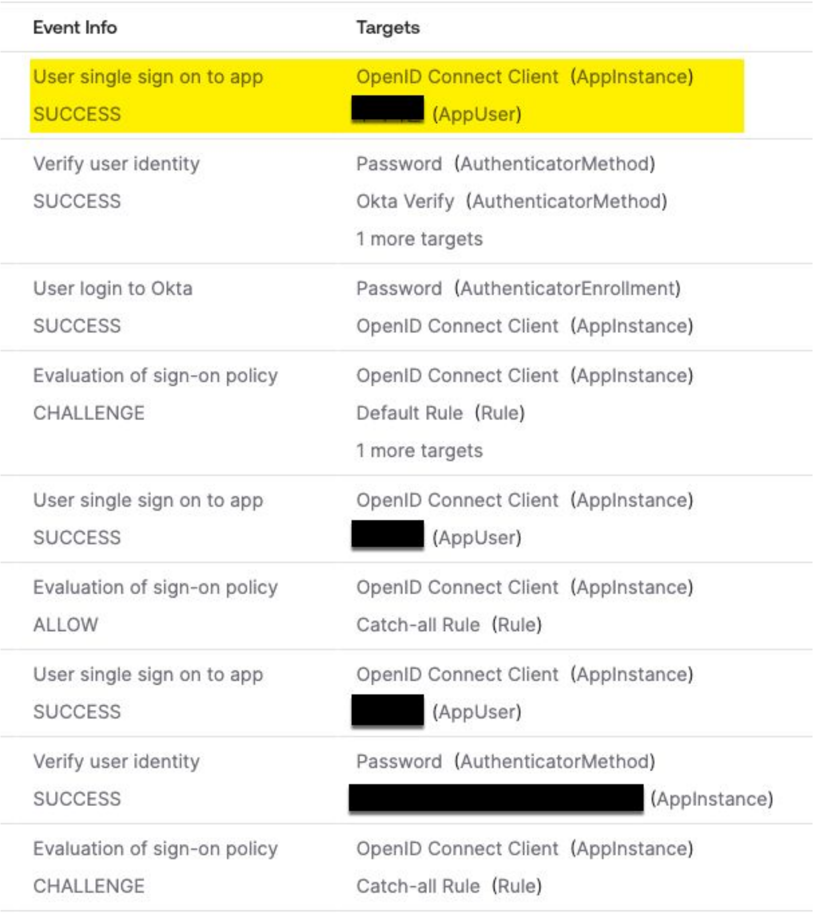
me	Status
[redacted]	302
authorize?client_id=0oajumpw2jMlrPZIr5d7&redirect_...l%2FUECDQTYpUvJdMEqz0...	200
[redacted]	200
okta-sign-in.min.js	200
okta-sign-in.min.css	200
loginpage-theme.c8c15f6857642c257bcd94823d968bb1.css	200
style-sheet?touch-point=SIGN_IN_PAGE&v=f991ebb043f...b8969a14da06b2d45c27...	200
default.6770228fb0dab49a1695ef440a5279bb.png	200
okta-logo.1e146cad5713da744492be95eb0f7793.png	200
initLoginPage.pack.58de3be0c9b511a0fdfd7ea4f69b56fc.js	200
Aeonik-Regular.c672e6fbaa411f5719f3.woff2	200
Inter-Regular.c8ba52b05a9ef10f4758.woff2	200
iframe.html	200
introspect	200
favicon.ico	200
discoveryIframe-17abdf702560067430e5.min.js	200
checkbox-sign-in-widget.png	200
Inter-SemiBold.b5f0f109bc88052d4000.woff2	200
okticon.woff	200
montserrat-okta-light-webfont.woff	200
montserrat-okta-regular-webfont.woff	200
devicefingerprint	200
fingerprint2.min.68ab45bd98459cb766f3ab26d086e5f5.js	200
crypto-js.eac8c800a39bc533f58390e6c0eef9bf.js	200
jquery-1.12.4.2ef93d9aedc4198ec425a799a371292d.js	200
nonce	200
identify	200
oktaVerify_70x70.png	200
user-icon.svg	200
answer	200
sign-on-widget-spinner.gif	200
redirect?stateToken=02.id.eNFGgP[redacted]NiA1z3btz	302
idpresponse?code=J[redacted]ubUF...l%2FUECDQTYpUvJdM...	302
[redacted]	(failed) net::ERR_HTTP_RESPONSE_CODE_FAILURE
data:image/png;base...	200
data:image/png;base...	200
data:image/png;base...	200

[redacted]에 대한 액세스가 거부됨

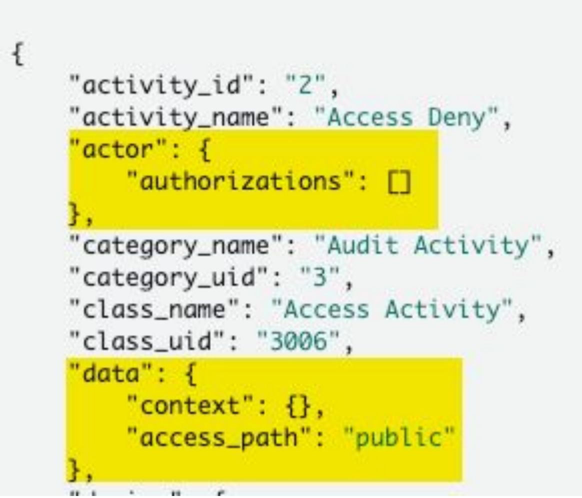
이 페이지를 볼 수 있는 권한이 없습니다.

HTTP ERROR 403

Troubleshooting

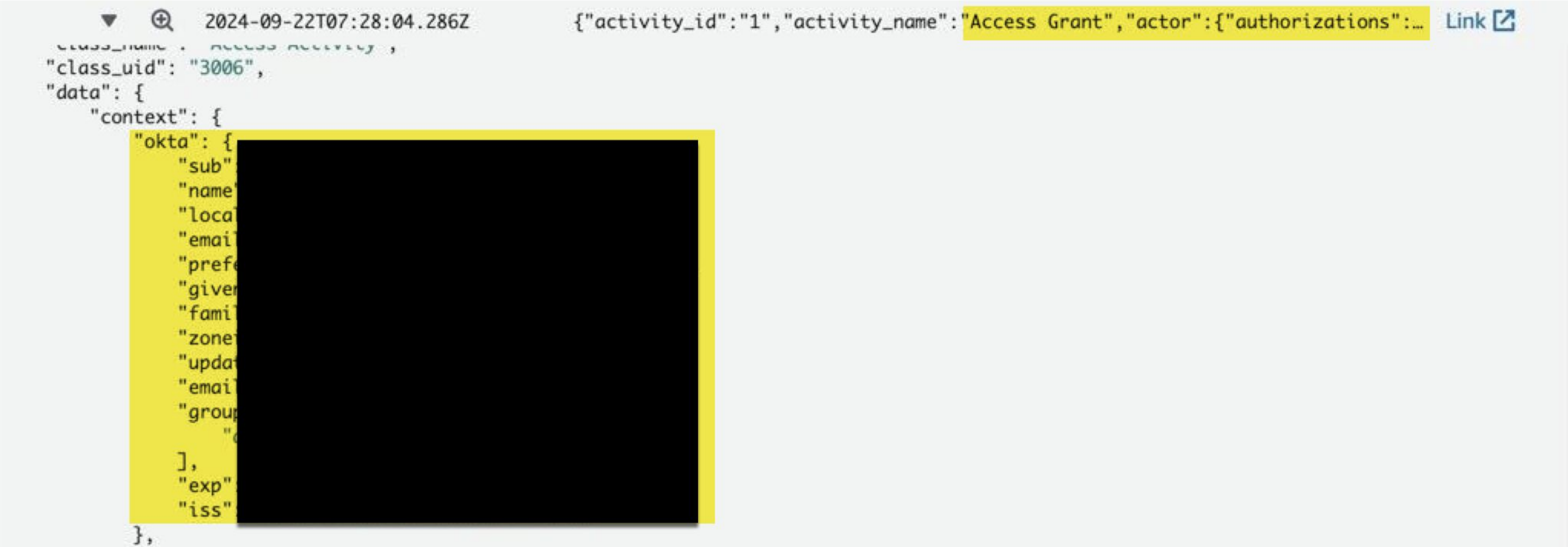


Event Info	Targets
User single sign on to app SUCCESS	OpenID Connect Client (AppInstance) [redacted] (AppUser)
Verify user identity SUCCESS	Password (AuthenticatorMethod) Okta Verify (AuthenticatorMethod) 1 more targets
User login to Okta SUCCESS	Password (AuthenticatorEnrollment) OpenID Connect Client (AppInstance)
Evaluation of sign-on policy CHALLENGE	OpenID Connect Client (AppInstance) Default Rule (Rule) 1 more targets
User single sign on to app SUCCESS	OpenID Connect Client (AppInstance) [redacted] (AppUser)
Evaluation of sign-on policy ALLOW	OpenID Connect Client (AppInstance) Catch-all Rule (Rule)
User single sign on to app SUCCESS	OpenID Connect Client (AppInstance) [redacted] (AppUser)
Verify user identity SUCCESS	Password (AuthenticatorMethod) [redacted] (AppInstance)
Evaluation of sign-on policy CHALLENGE	OpenID Connect Client (AppInstance) Catch-all Rule (Rule)



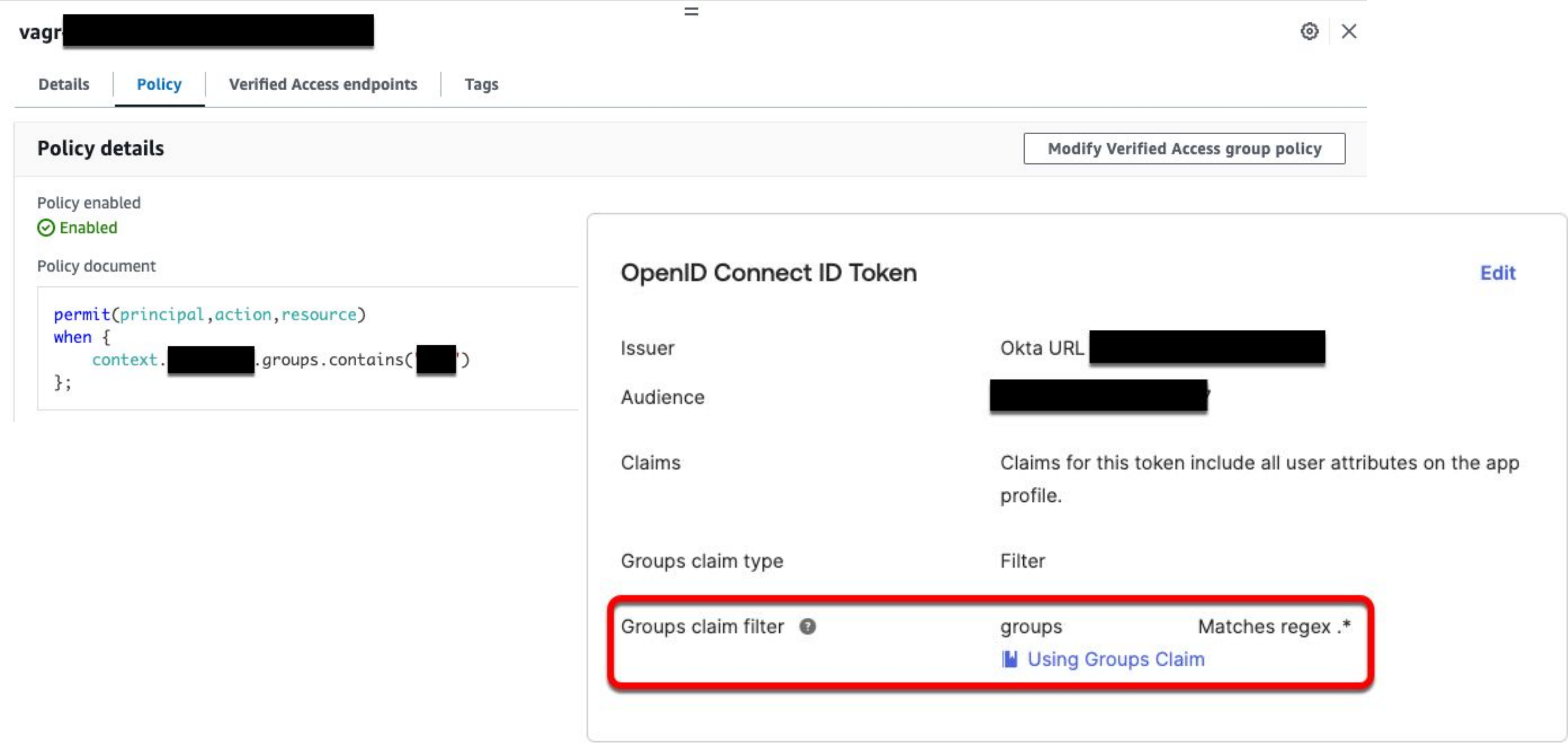
```
{
    "activity_id": "2",
    "activity_name": "Access Deny",
    "actor": {
        "authorizations": []
    },
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "data": {
        "context": {},
        "access_path": "public"
    },
```

Troubleshooting



```
▼  2024-09-22T07:28:04.286Z   {"activity_id":"1","activity_name":"Access Grant","actor":{"authorizations":…  Link
 "class_name": "Access Activity",
 "class_uid": "3006",
 "data": {
     "context": {
         "okta": { [redacted]
             "sub"
             "name'
             "loca
             "emai
             "pref
             "giver
             "fami
             "zone
             "upda
             "emai
             "grou
                 "
             ],
             "exp"
             "iss"
         },
```

Troubleshooting



vagr[redacted]

Details
Policy
Verified Access endpoints
Tags

Policy details

Modify Verified Access group policy

Policy enabled
✓ Enabled

Policy document

```
permit(principal,action,resource)
when {
    context.[redacted].groups.contains([redacted]')
};
```

OpenID Connect ID Token

Issuer: Okta URL [redacted]

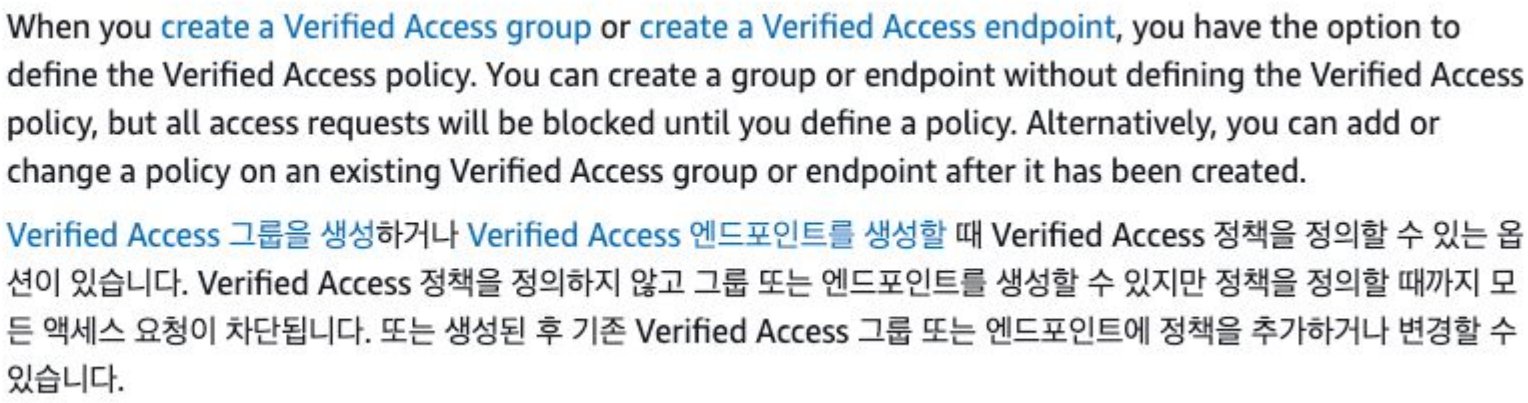
Audience: [redacted]

Claims: Claims for this token include all user attributes on the app profile.

Groups claim type: Filter

Groups claim filter: groups Matches regex .*

Troubleshooting

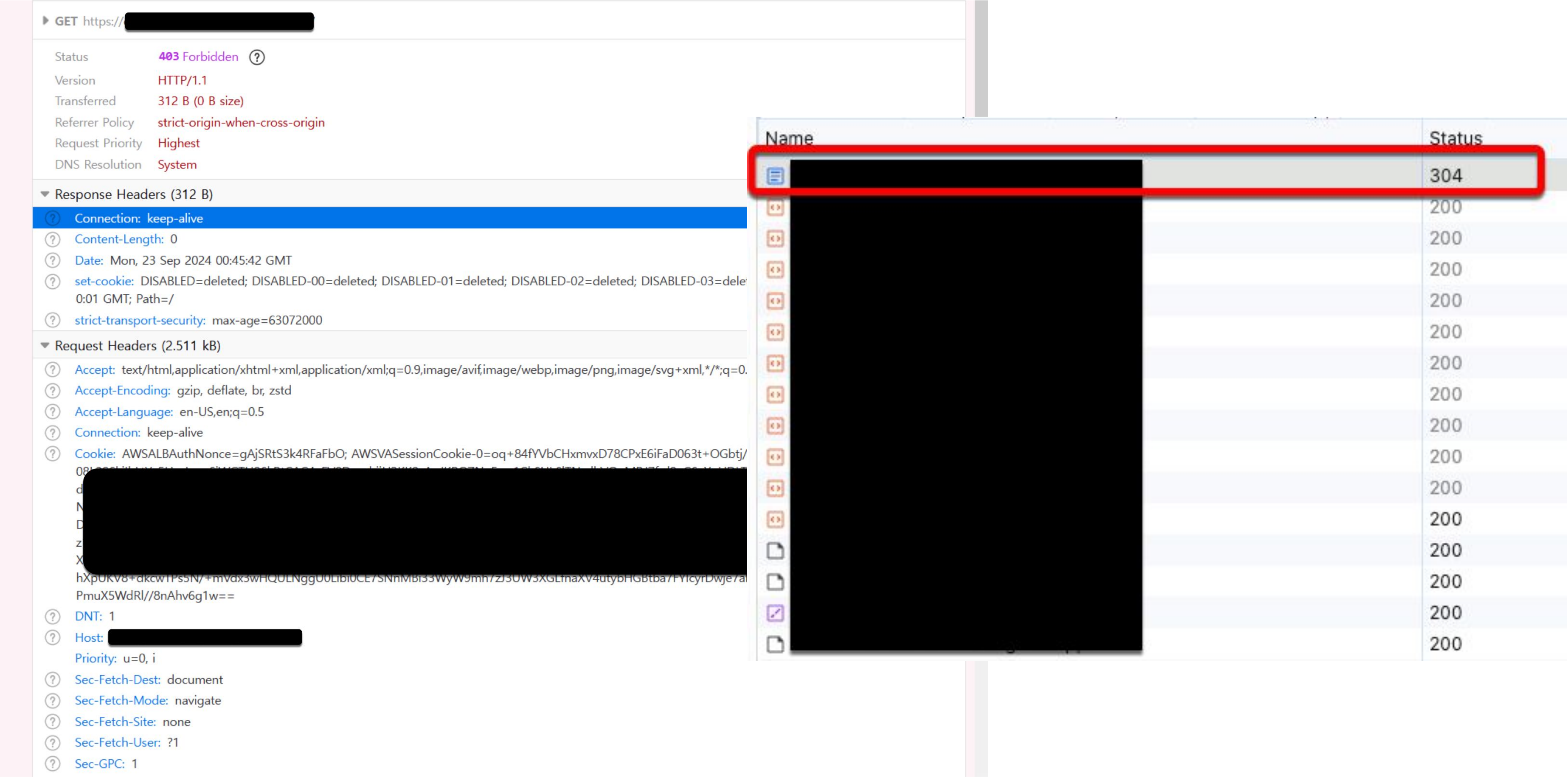


When you create a Verified Access group or create a Verified Access endpoint, you have the option to define the Verified Access policy. You can create a group or endpoint without defining the Verified Access policy, but all access requests will be blocked until you define a policy. Alternatively, you can add or change a policy on an existing Verified Access group or endpoint after it has been created.

Verified Access 그룹을 생성하거나 Verified Access 엔드포인트를 생성할 때 Verified Access 정책을 정의할 수 있는 옵션이 있습니다. Verified Access 정책을 정의하지 않고 그룹 또는 엔드포인트를 생성할 수 있지만 정책을 정의할 때까지 모든 액세스 요청이 차단됩니다. 또는 생성된 후 기존 Verified Access 그룹 또는 엔드포인트에 정책을 추가하거나 변경할 수 있습니다.

출처 : Verified Access policies

Troubleshooting



GET https://[redacted]

Status	403 Forbidden ?
Version	HTTP/1.1
Transferred	312 B (0 B size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest
DNS Resolution	System

Response Headers (312 B)

```
Connection: keep-alive
Content-Length: 0
Date: Mon, 23 Sep 2024 00:45:42 GMT
set-cookie: DISABLED=deleted; DISABLED-00=deleted; DISABLED-01=deleted; DISABLED-02=deleted; DISABLED-03=dele
0:01 GMT; Path=/
strict-transport-security: max-age=63072000
```

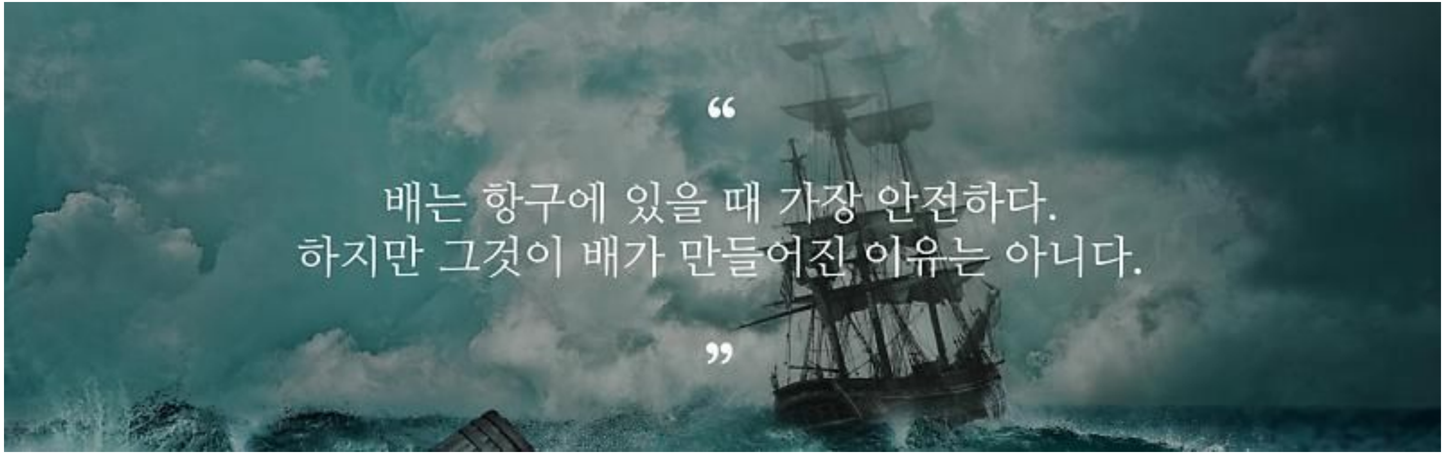
Request Headers (2.511 kB)

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: AWSALBAuthNonce=gAjSRtS3k4RFaFbO; AWSVASessionCookie-0=oq+84fYVbCHxmvxD78CPxE6iFaD063t+OGbtj/
[redacted]
PmuX5WdRl//8nAhv6g1w==
DNT: 1
Host: [redacted]
Priority: u=0, i
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Sec-GPC: 1
```

Name	Status
[redacted]	304
	200
	200
	200
	200
	200
	200
	200
	200
	200
	200
	200
	200
	200
	200
	200

마치며.

보안은 서비스를 안전하게 하는 것이 목적이다.



“

배는 항구에 있을 때 가장 안전하다.
하지만 그것이 배가 만들어진 이유는 아니다.

”

Q&A

Appendix.

- AWS Verified Access Integration with 3rd party identity providers

- Integrating AWS Verified Access with device trust providers

- What is AWS Verified Access?

- CEDAR PLAYGROUND

- Exceed the 100 groups limitation on a group claim when using the Implicit Flow.