

DB 자격증명 개선 사례 공유

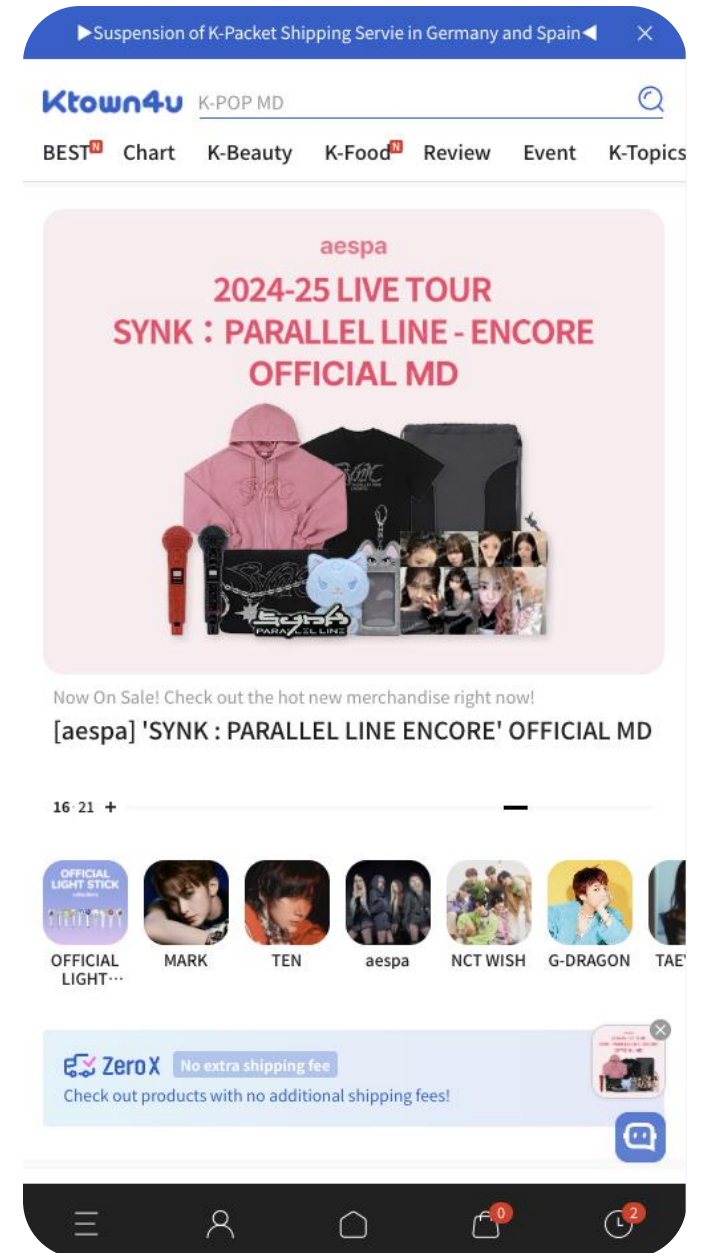


구경열

AWS classroom staff

FinOps Korea staff

Ktown4u DevOps Engineer



개요

**당신의 DB
안전하십니까?**



ID/PW

▼ Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB instance.

1 to 32 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

☐ **Managed in AWS Secrets Manager - *most secure***
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

☒ **Self managed**
Create your own password or have RDS create a password that you manage.

☐ **Auto generate password**

Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Password strength

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

Confirm master password [Info](#)

장점

- 간단하고 보편적임
- 운영의 친숙함

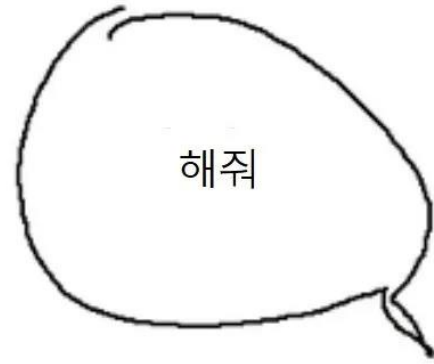


유지관리 어려움

단점

- 암호 회전 어려움
- SPOF
- 보안에 취약함

암호를 자동으로
관리해주면 좋겠다



Secrets Manager

▼ Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB instance.

admin

1 to 32 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.



Managed in AWS Secrets Manager - *most secure*

RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.



Self managed

Create your own password or have RDS create a password that you manage.



If you manage the master user credentials in AWS Secrets Manager, additional charges apply. See [AWS Secrets Manager pricing](#). Additionally, some RDS features aren't supported. See limitations [here](#).

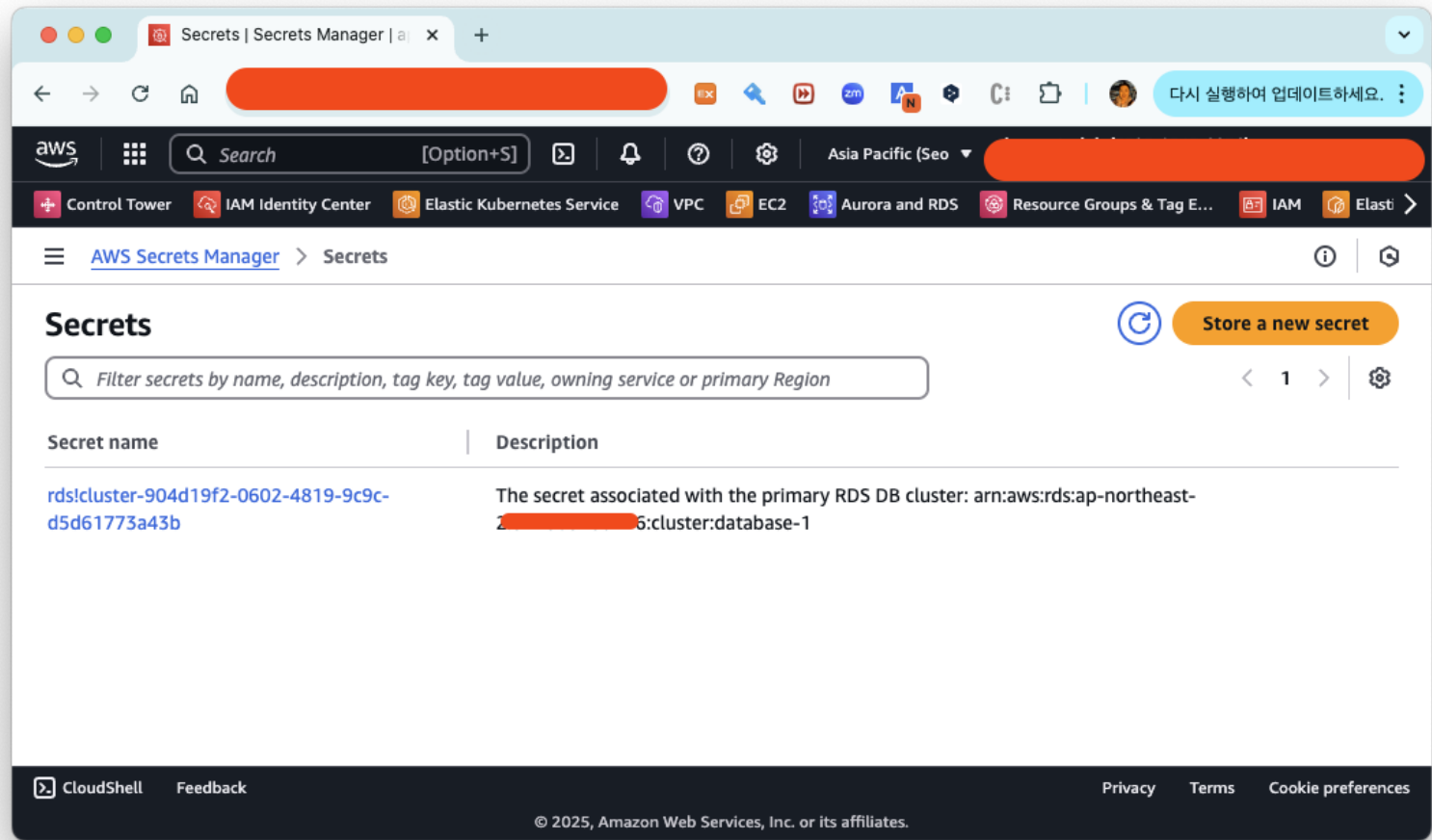
Select the encryption key [Info](#)

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

aws/secretsmanager (default)



[Add new key](#)



Overview

Rotation

Versions

Replication

Tags

Rotation configuration [Info](#)

Rotate secret immediately

Edit rotation

Rotation status

✓ Enabled

Rotation schedule

rate(4 hours)

Last rotated date (UTC)

Mon, April 7, 2025 at 13:25:16 UTC

Next rotation date (UTC)

The next rotation is scheduled to occur on or before this date.

Mon, April 7, 2025 at 17:59:59 UTC

Secret value [Info](#)

Retrieve and view the secret value.

Key/value

Plaintext

Secret key

Secret value

username

 admin

password

 :4~NX7xdxI5CCTq<(P*[giQ.C[c>

Secret value [Info](#)

Retrieve and view the secret value.

Key/value

Plaintext

Secret key

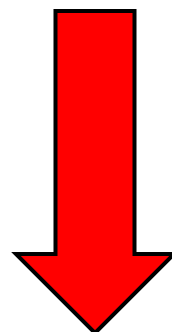
Secret value

username

 admin

password

 V06>mMX8:dz6cYW4iYz4)soR?.(P



장점

- 암호 관리할 필요가 없음
- 주기적인 암호 회전
- 필요시 즉각적으로 암호 회전



이게 최선 ?

단점

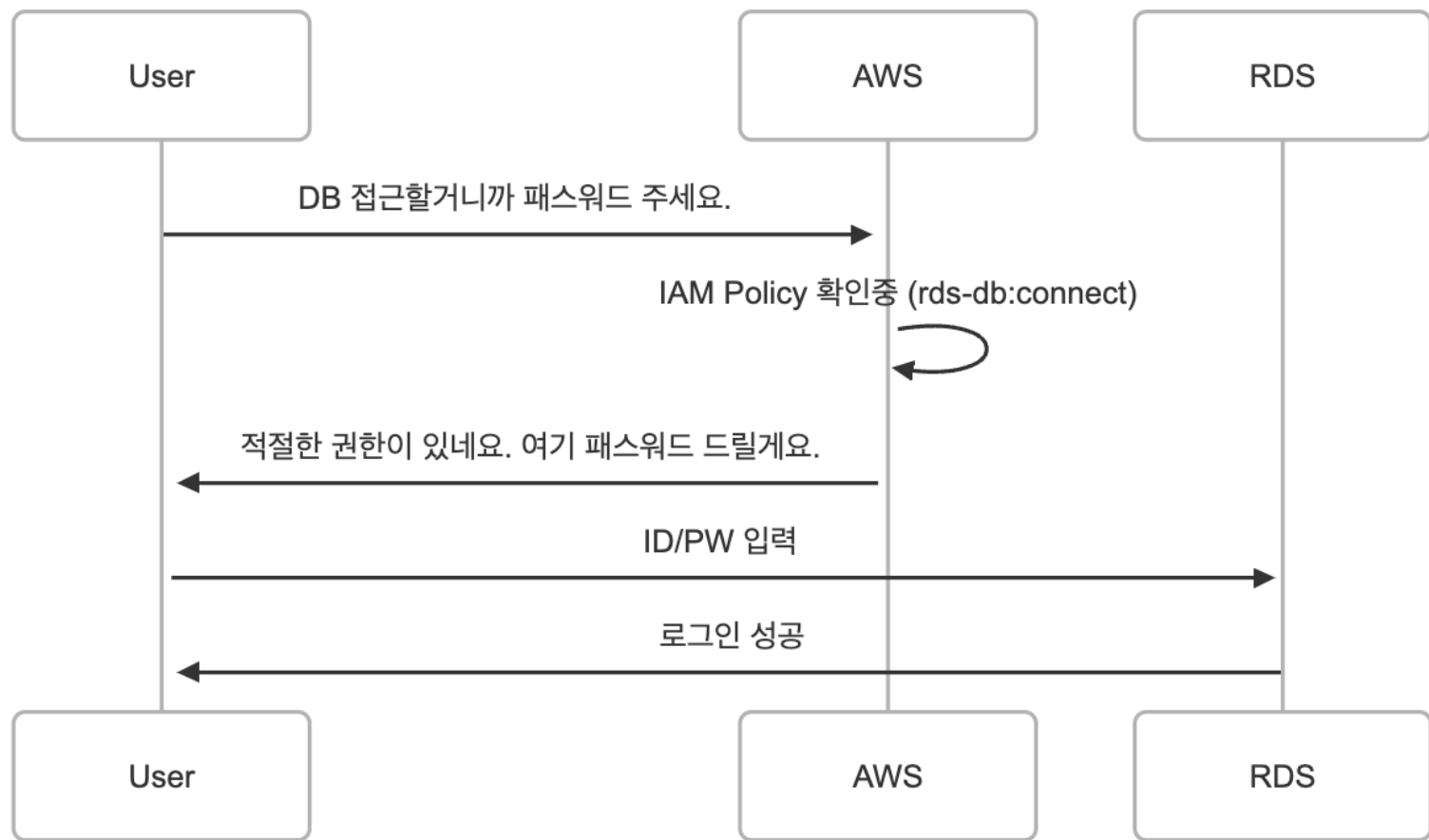
- Secrets Manager 의존성 발생
- Secrets Manager 접근 권한 필요
- 비용 발생



행!복! 해줘~

IAM Auth

작동 방식




Bash

 Copy

개발 DB 접근

RDSHOST=".ap-northeast-2.rds.amazonaws.com"

USERNAME=""

REGION="ap-northeast-2"

TOKEN="\$(aws rds generate-db-auth-token --hostname \$RDSHOST --port 3306 --region ap-northeast-2 --username \$USERNAME)"

mysql \

 --host=\$RDSHOST \

 --port=3306 \

 --ssl-ca=ap-northeast-2-bundle.pem \

 --enable-cleartext-plugin --user=\$USERNAME \

 --password=\$TOKEN

장점

- 암호 관리할 필요가 없음
- 항상 새로운 암호
- IDE에서도 사용이 쉬움

단점

- Hostname 변경 불가
- DB에서 추가적인 메모리 사용
- 연결 제한 (초당 200건)

사례

누가 DB User를 사용하고 있는가?

누가 DB User를 사용하고 있는가?

개발자 (사람)

애플리케이션 (서비스)

AWS Identity Center + IAM Auth 활용

AWS Identity Center + IAM Auth 활용

- AWS SSO 로그인 계정을 DB 계정과 통합
- 자신의 계정만 접근가능 해야함
- 매번 암호를 입력하면 번거로움

AWS Identity Center + IAM Auth 활용



Settings

Details
Configure your Identity source and multi-factor authentication settings for use when managing access to your AWS accounts, resources, and

Instance name - [Edit](#)
ktown4u

Region
Asia Pacific (Seoul) | ap-northeast-2

Delegated administrator
 Registered account: management

Date created
Thursday, October 24, 2024 at 3:51:54 PM GMT+9

Identity-aware sessions - [Enable](#)
 Disabled

Enable identity-aware sessions
Identity-aware sessions provide personalized experiences for users of AWS managed applications. Identity-aware sessions are required for Developer in the console. [Learn about identity-aware sessions](#)

Identity source

Authentication

Attributes for access control

Management


Tags

Attributes for access control (2)
Assign access to workforce users and groups based on key-value pairs that you identify for a specific incoming attribute. [Learn more](#)

Find attributes

Key	Value
Department	\${path:enterprise.department}
username	\${path:userName}

AWS Identity Center + IAM Auth 활용

 [IAM Identity Center](#) > [Settings](#)

IAM Identity Center <


Settings

Details


Configure your Identity source and multi-factor authentication settings for use when managing access to your AWS accounts, resources, and



Instance name - [Edit](#)
ktown4u

Region
Asia Pacific (Seoul) | ap-northeast-2

Delegated administrator
 [Registered account: management](#)

Date created
Thursday, October 24, 2024 at 3:51:54 PM GMT+9

Identity-aware sessions - [Enable](#)
 Disabled

 **Enable identity-aware sessions**
Identity-aware sessions provide personalized experiences for users of AWS managed applications. Identity-aware sessions are required for Developer in the console. [Learn about identity-aware sessions](#) 

Identity source


Authentication

Attributes for access control

Management

Tags

Attributes for access control (2)

Assign access to workforce users and groups based on key-value pairs that you identify for a specific incoming attribute. [Learn more](#) 

Key	Value
Department	<code>\${path:enterprise.department}</code>
username	<code>\${path:userName}</code>

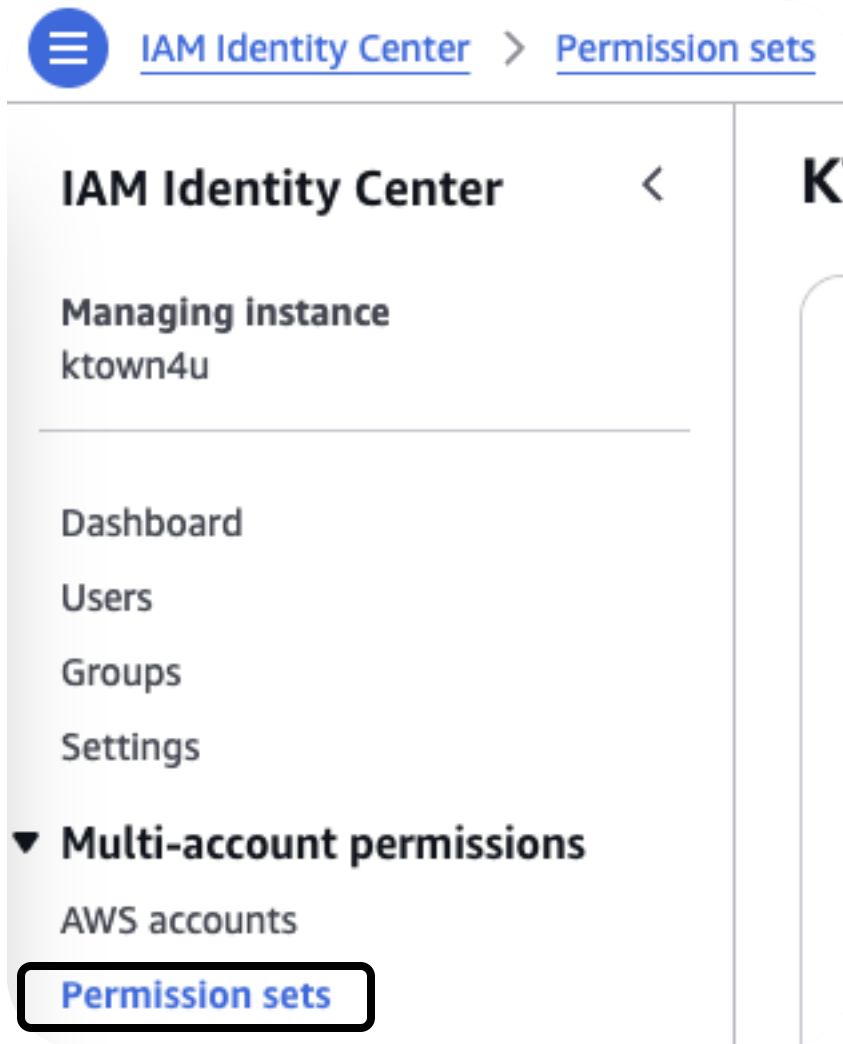
Supported external identity provider attributes

The following table lists all external identity provider (IdP) attributes supported in IAM Identity Center. When using SAML assertions, you can use whichever attribu

Supported attributes in your IdP
<code>\${path:userName}</code>
<code>\${path:name.familyName}</code>
<code>\${path:name.givenName}</code>
<code>\${path:displayName}</code>
<code>\${path:nickName}</code>
<code>\${path:emails[primary eq true].value}</code>
<code>\${path:addresses[type eq "work"].streetAddress}</code>
<code>\${path:addresses[type eq "work"].locality}</code>
<code>\${path:addresses[type eq "work"].region}</code>
<code>\${path:addresses[type eq "work"].postalCode}</code>
<code>\${path:addresses[type eq "work"].country}</code>
<code>\${path:addresses[type eq "work"].formatted}</code>
<code>\${path:phoneNumbers[type eq "work"].value}</code>
<code>\${path:userType}</code>
<code>\${path:title}</code>
<code>\${path:locale}</code>
<code>\${path:timezone}</code>
<code>\${path:enterprise.employeeNumber}</code>
<code>\${path:enterprise.costCenter}</code>
<code>\${path:enterprise.organization}</code>
<code>\${path:enterprise.division}</code>
<code>\${path:enterprise.department}</code>
<code>\${path:enterprise.manager.value}</code>



AWS Identity Center + IAM Auth 활용



```
{  
  "Sid": "DBAccess",  
  "Effect": "Allow",  
  "Action": [  
    "rds-db:connect"  
  ],  
  "Resource": "arn:aws:rds-db:*:*:dbuser:*/${aws:PrincipalTag/username}"  
},  
}
```

SSO ID AND DB User : kyungyeol.gu@ktown4u.com

AWS Identity Center + IAM Auth 활용

```
{  
  "Sid": "DBAccess",  
  "Effect": "Allow",  
  "Action": [  
    "rds-db:connect"  
  ],  
  "Resource": "arn:aws:rds-db:*:*:dbuser:*,  
  "${aws:PrincipalTag/username}"  
},
```

Identity source | Authentication | **Attributes for access control** | Management | Tags

Attributes for access control (2)
Assign access to workforce users and groups using key-value pairs that you identify for a specific incoming attribute. [Learn more](#)

Find attributes

Key	Value
Department	\${path:enterprise.department}
username	\${path:userName}

Identity Center username