Headline

Strategy for implementing major ISMS certification items in AWS cloud environment

Manager, Public Consulting/Enhancement Team, Shin Gwan-yong

■ Outline

Source: Korea Internet & Security Agency (KISA) website

Recently, when building IT infrastructure, an increasing number of companies are switching from an on-premise environment to a cloud environment or taking a hybrid approach. According to a market research company IDC, the size of the global cloud market last year was KRW850 trillion, up by 20% over the previous year, and is expected to grow at an average annual rate of 19.4% over the next five years, reaching KRW1,733 trillion by 2027.

The cloud environment helps effectively store large amounts of data generated through digital transformation. Through this cloud environment, companies can secure business competitiveness by increasing availability and scalability, reducing costs and improving efficiency. In particular, when using cloud services, flexible response is possible even in unexpected emergency situations. So it is used more widely now.

It is necessary for companies to establish and manage security policies to meet the requirements for protection measures in a cloud environment. However, compared to the security policy and service provided by the cloud service provider (CSP), the terminology and components are different. So security managers are experiencing many difficulties.

Therefore, in this Insight, in order to provide help to managers preparing for ISMS (Information Security Management System) certification in a cloud environment, we would like to suggest an implementation method for major ISMS certification items in the Amazon web service (AWS) cloud environment, which has the most users worldwide.

■ Matching technical certification items of ISMS requirements for protection measures and services provided within AWS

ISMS certification is Korea's most authoritative information protection and management system certification jointly announced by the Ministry of Science and ICT and the Personal Information Protection Committee. To receive ISMS certification, a total of 80 certification criteria – establishment and operation of the management system (16 items) and requirements for protection measures (64 items) – must be met, as well as the adequacy of 234 detailed inspection items. Companies that have acquired ISMS certification are evaluated as companies capable of responding quickly to hacking and personal information leaks.

First, technical certification items of ISMS requirements for protection measures and services provided within AWS are as follows:

ISMS item	Services provided within AWS
2.1 Policy, organization and asset management	N/A
2.2 Personnel security	
2.3 Outsider security	
2.4 Physical security	
2.5 Certification and authorization management	**IAM**
2.6 Access control	**VPC**
2.7 Application of encryption	**Key Management Service**
2.8 Introduction of data system and development security	N/A
2.9 System and service operation management	**CloudTrail, CloudWatch AWS System Manager**
2.10. System and service security management	**AWS WAF, AWS Firewall**
2.11. Incident prevention and response	N/A
2.12 Disaster recovery	

Source: Guide to ISMS-P certification criteria reprocessed

Table 1. Matching ISMS requirements for protection measures and services provided within AWS

■ How to implement major certification items

1. ISMS certification items – 2.5 Certification and authorization management

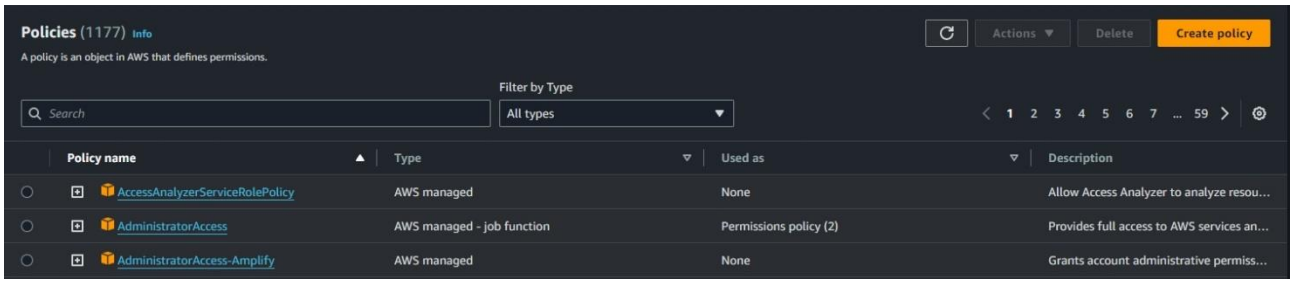
1) 2.5.1 User account management / 2.5.2 User identification / 2.5.6 Review access permissions

Accounts used in AWS services include the root user account and the IAM user account.

- AWS root account: As it is a superuser account that can access all AWS services and resources, it is not recommended to use it when operating the service.
- AWS IAM (Identity and Access Management): Account management service, e.g., authentication (login) and authorization to create an account that accesses AWS services

※ Service-specific (EC2, RDS) accounts are managed by each service.

Basically, account creation/management is performed through IAM. Account permissions can be granted by user and group, and AWS provides pre-defined permissions for the top manager/each administrator/user for each service through the 'managed policy'. Also, you can create your own policy and grant desired permissions.

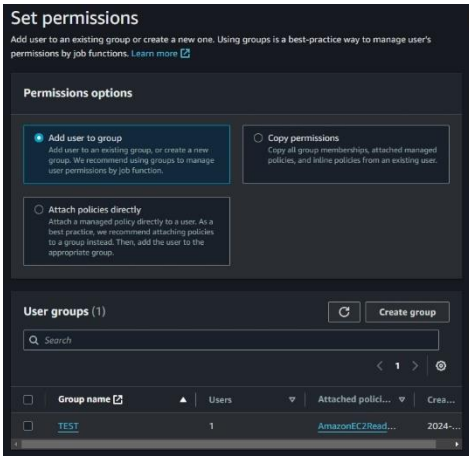


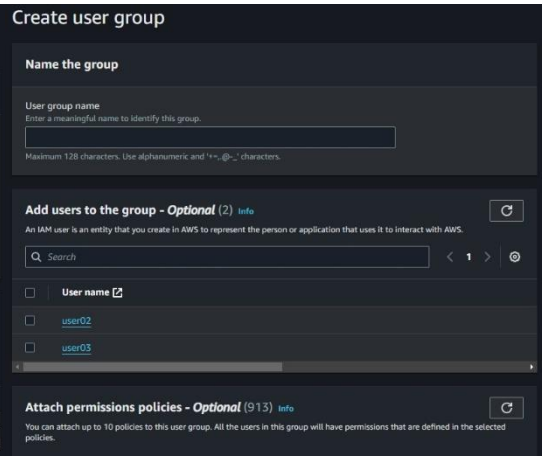
Source: AWS console website

Figure 1. Managed policy provided by AWS

★ Key Point

When using a small number of accounts, you can manage them by granting permissions to each account. However, if you are creating multiple accounts, it is easier to create groups for each job and then grant permissions during management/review of permissions.





Source: AWS console website

Figure 2. Creating a user group

Figure 3. Authorizing by designating a group

2) 2.5.3 User authentication

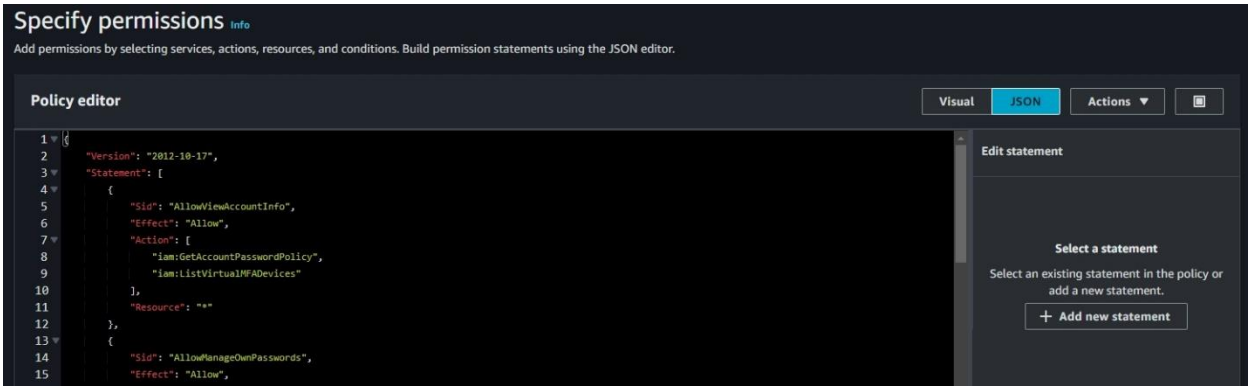
Accounts accessing personal information and important information must apply secure authentication procedures. AWS provides three types of MFA (Multi Factor Authentication).

- Mobile OTP authentication: OTP generation and authentication with the Google Authenticator APP
- FIDO secure key authentication: Authentication using security keys that support FIDO standards
- Hardware OTP authentication: Authentication using the hardware-based OTP generator

★ Key Point

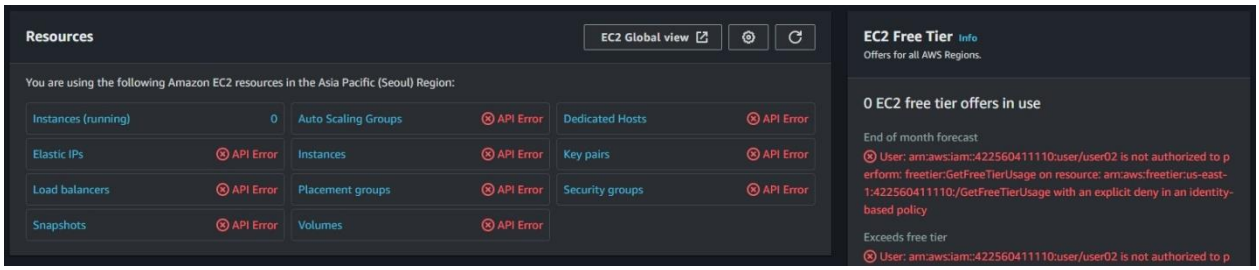
If MFA is not set after a user account is created, the IAM policy can be applied by force to prevent access to AWS services. You can refer to the AWS document below to create a forced MFA authentication policy and then apply the policy directly to the group policy or user.

※ Reference link: https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/tutorial_users-self-manage-mfa-and-creds.html



Source: AWS console website

Figure 4. IAM Creating the forced MFA authentication policy through the JSON editor when creating the IAM policy



Source: AWS console website

Figure 5. When the forced MFA authentication policy is applied, use of AWS services is restricted until MFA is enabled

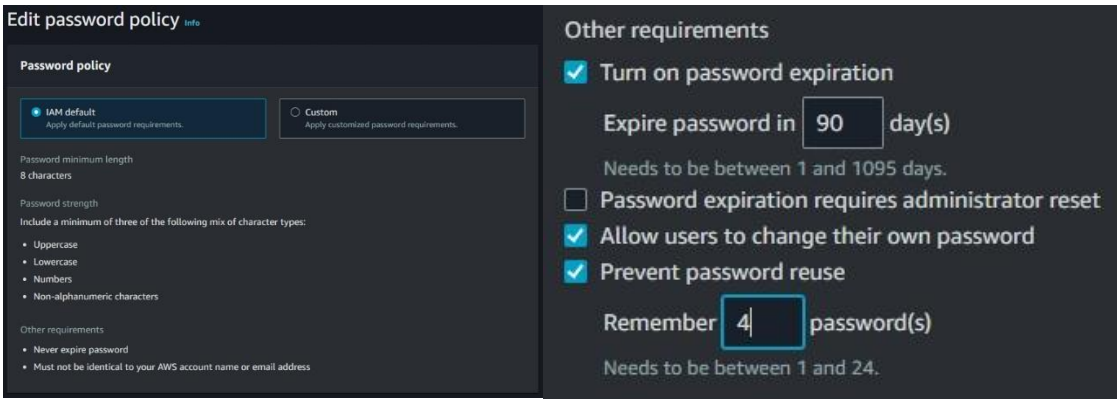
3) 2.5.4 Password management

The default password management rules in AWS are as follows:

- Minimum password length: eight characters
- At least three of upper/lowercase letters, numbers, and special characters must be included.
- Use of the same characters as the AWS account name or e-mail address is prohibited.
- Login is limited for five seconds when the password fails ten times.

Rules other than the default values must be set manually as follows:

- Password expiration period setting: 90 days or less
- Allowing users to change their own password: Enable Allow
- Limiting password reuse: Reuse of the same password is limited, and it is recommended to memorize four or more.



Source: AWS console website

Figure 6. Default password policy　　Figure 7. Additionally provided password policy

★ Key Point

Source: AWS console website

Figure 8. Initial user password forced change option

When initially granting an account to an IAM user or initializing a password, the administrator must directly check the above option to change the initial password by force.

4) 2.5.5 Special account and authorization management

Among the policies that can be set in AWS IAM, special permissions (administrator permissions) are as follows:

Policy name	Description
AdministratorAccess	Provides full access to AWS services and resources ※ Minimum permissions should be granted to only those accounts which you will grant permissions to as chief administrator instead of the root account.
FullAccess	Provides full access to each service (EC2, RDS, S3, etc.) ※ Since resource creation/deletion/modification is possible for each service, minimum permissions should be granted only to those accounts which perform relevant jobs.

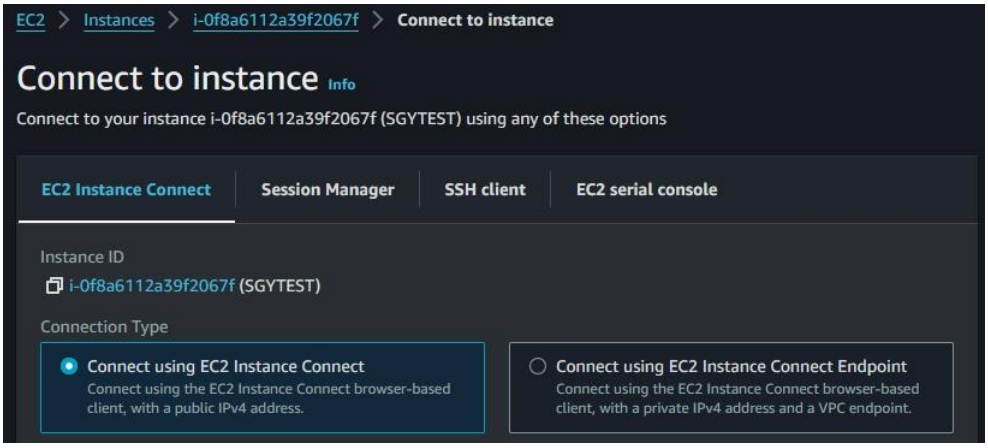
Source: AWS guide website reprocessed

Table 2. AWS IAM administrator permissions policy

★ Key Point

If you have AdministratorAccess or Ec2FullAccess permissions, you can directly access the EC2 instance using the EC2 instance direct access function without using SSH. To restrict bypass access other than SSH, you must remove the ec2-instance-connect package within the EC2 instance by referring to the link below.

※ Reference link: https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/ec2-instance-connect-uninstall.html



Source: AWS console website

Figure 9. Direct connection to the EC2 instance provided in AWS

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

Source: AWS guide website

Figure 10. Removal of ec2-instance-connect from the EC2 instance

2. ISMS certification items – 2.6 Access control

1) 2.6.1 Network access / 2.6.7 Internet access control

In AWS, an independent network called VPC (Virtual Private Cloud) is configured.

In VPC, the network area is divided into public and private.

- Public: The network area that can communicate with an external network through an Internet gateway
- Private: The network area allocated as a private IP and capable of communicating only over the internal network

Instances operated for external services such as WEB service are allocated as public, and instances exclusively for internal networks that do not require external communication are allocated as private.

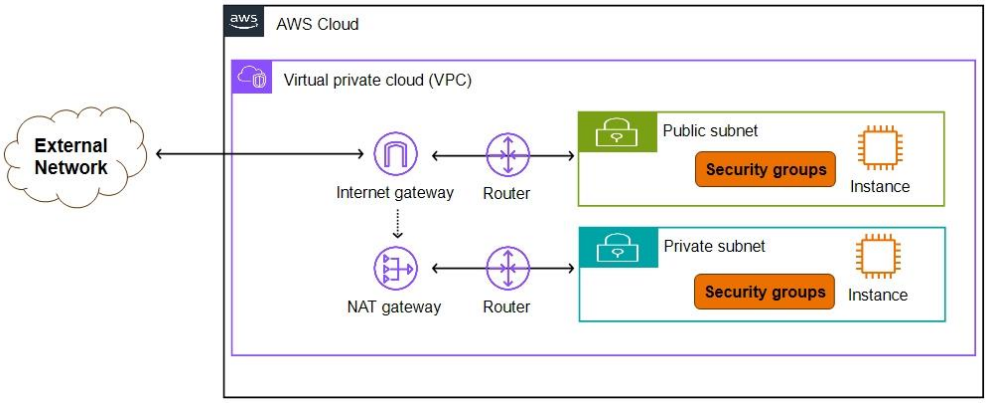


Figure 11. AWS network diagram

★ Key Point

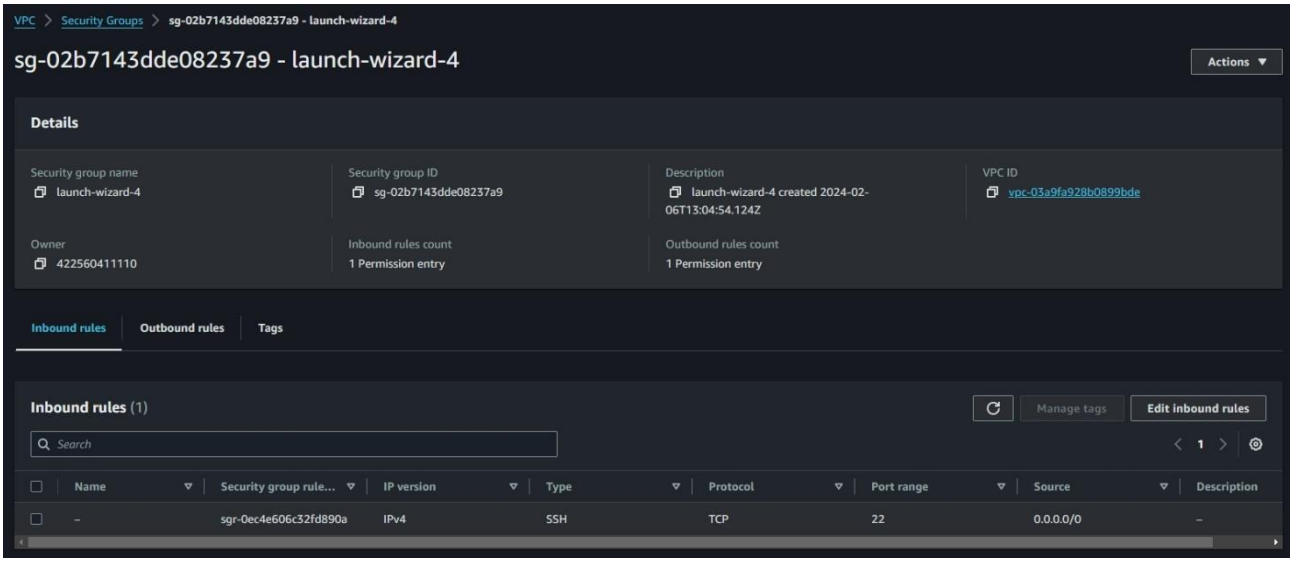
If you set public access when creating EC2, RDS, or S3 in AWS, instances/buckets will be able to communicate directly with an external network regardless of routing and can be accessed directly. So it is not recommended to enable public access for instances/buckets.

Source: AWS console website

Figure 12. S3 bucket public access blocking settings

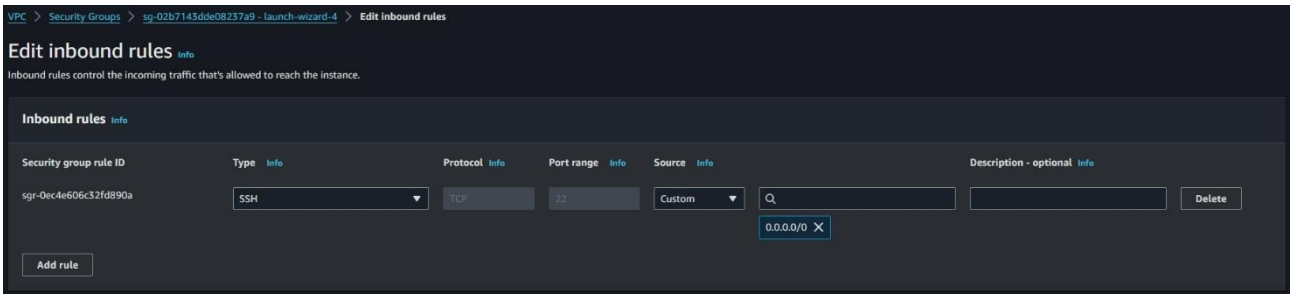
2) 2.6.2 Accessing the information system

AWS VPC provides a security group that acts as a firewall to control access to each instance. The security group works as ALL DENY if no policy is added, and is operated by registering IP/PORT policies that require permission.



Source: AWS console website

Figure 13. AWS security group



Source: AWS console website

Figure 14. Editing the AWS security group policy

★ Key Point

When a security group is first created, the SSH allow policy is set for inbound rules, and the allow all traffic policy is set for outbound rules by default. Therefore, after adding the IP/PORT policy that requires access, the default policy must be removed.

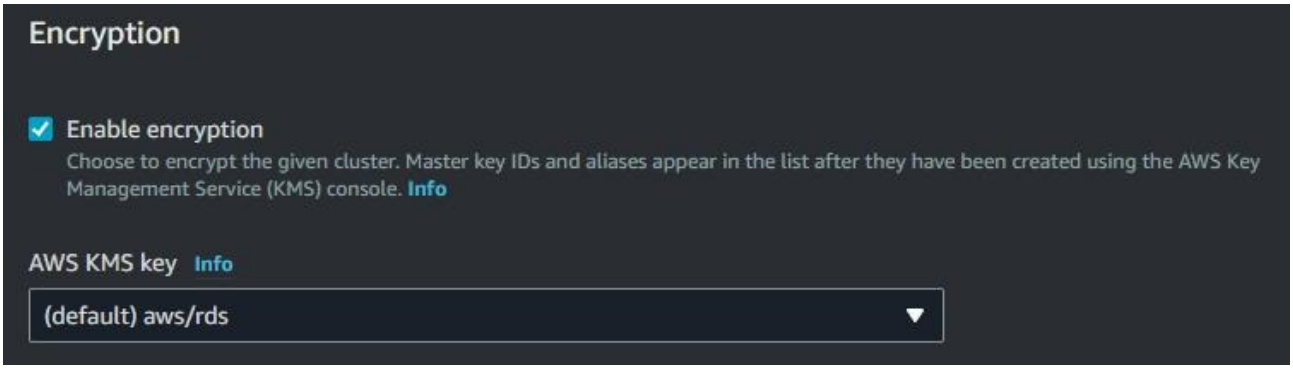
3. ISMS certification items – 2.7 Applying encryption

1) 2.7.1 Applying password policy / 2.7.2 Managing encryption key

You can set encryption for services where data is stored, e.g., EC2 storage, RDS, and S3. For EC2 and RDS, you can set whether to encrypt when creating an instance, and for S3 buckets, encryption using an S3 managed key will be automatically applied as the default value starting January 5, 2023.

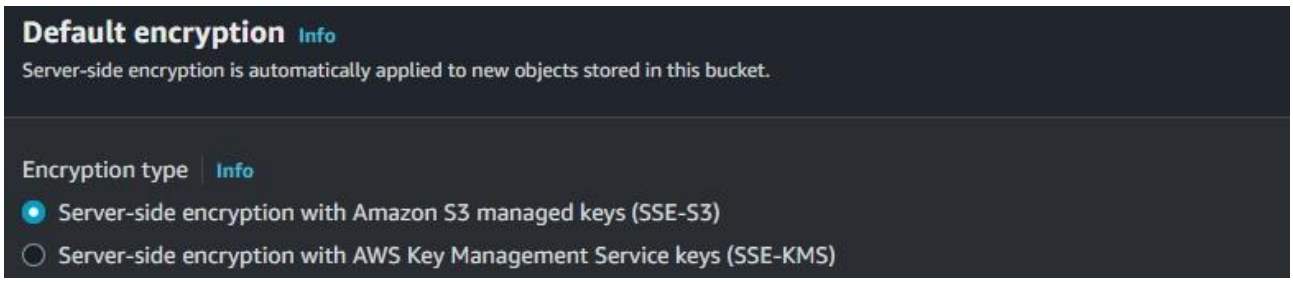
Source: AWS console website

Figure 15. EC2 storage encryption settings



Source: AWS console website

Figure 16. Encryption settings when RDS is created

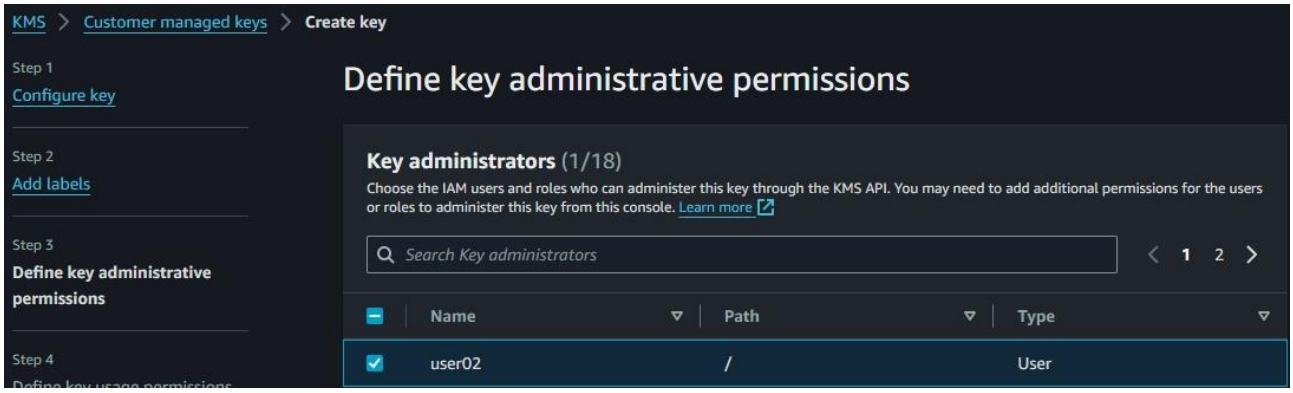


Source: AWS console website

Figure 17. S3 bucket encryption settings (default encryption is applied)

★ Key Point

To allow only specific users to access important data, you must create a key in Key Management Service, designate an account to use the key, and apply encryption.



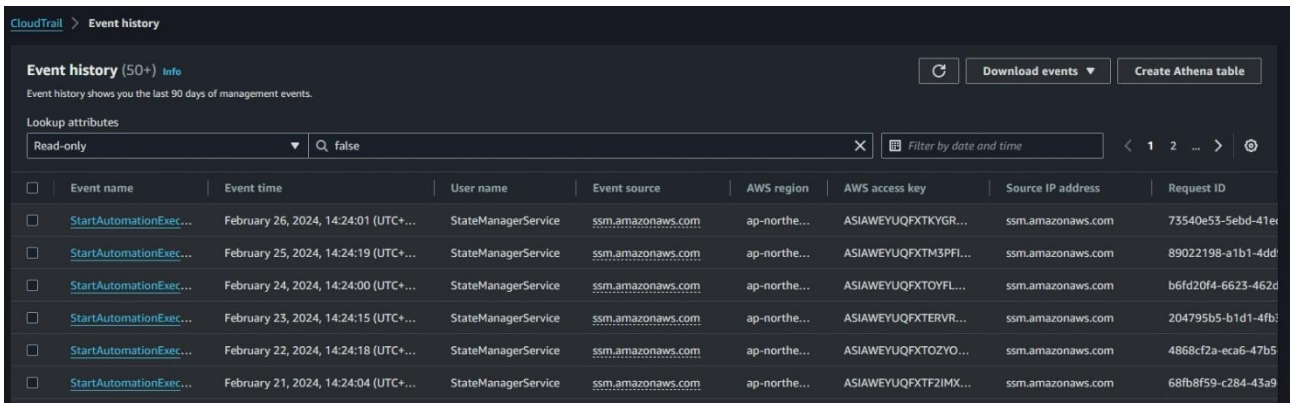
Source: AWS console website

Figure 18. User designation screen when creating a key in KMS

4. ISMS certification items – 2.9 System and service operation management

1) 2.9.4 Log and access record management

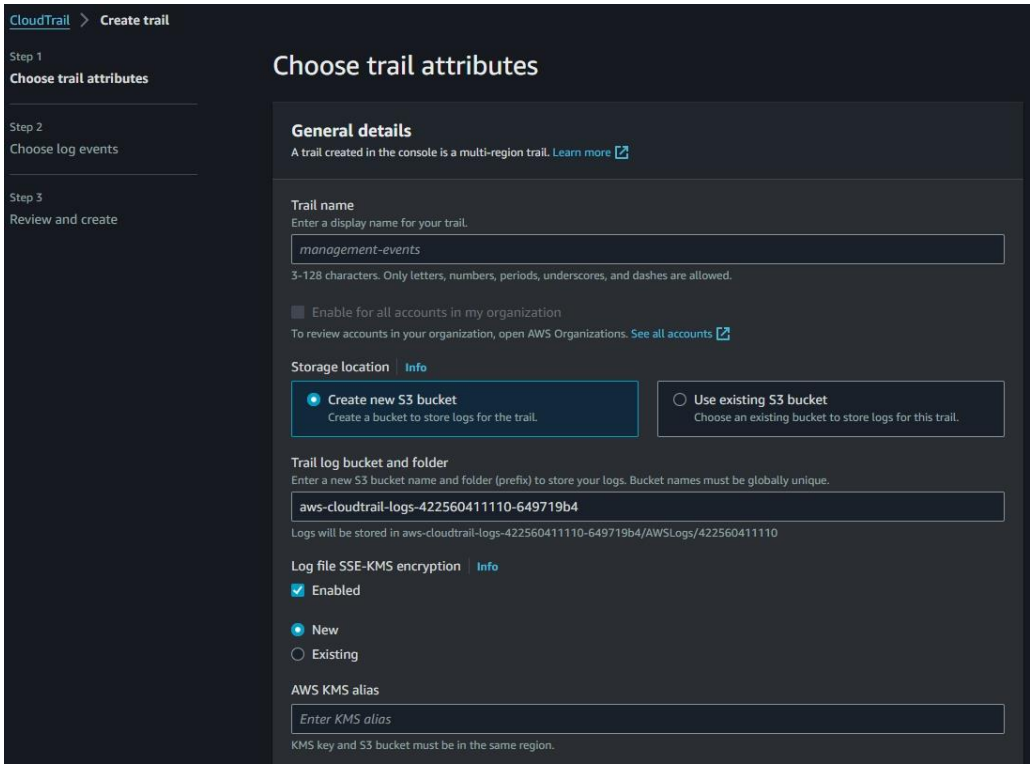
All activity logs in your AWS account are automatically recorded in CloudTrail. Event logs are stored for up to 90 days, and in order to store them for more than 90 days, you must create a trail and store it in an S3 bucket.



Source: AWS console website

Figure 19. AWS CloudTrail event records

You can create a trail and save CloudTrail event logs in an S3 bucket, and if you set SSE-KMS encryption, the logs will be encrypted and stored.

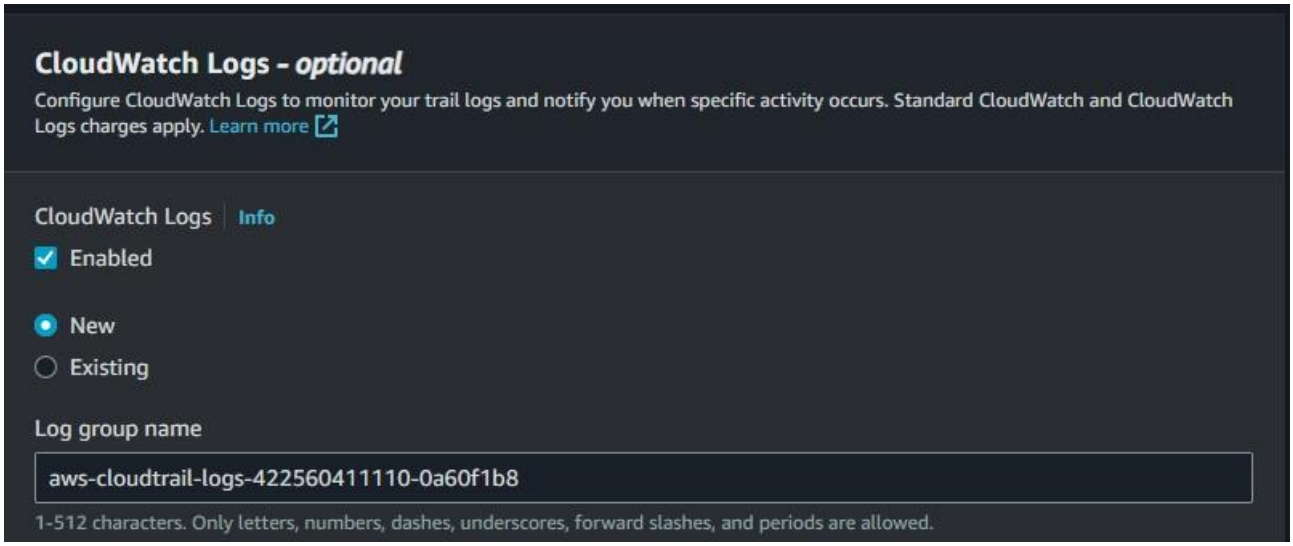


Source: AWS console website

Figure 20. Creating an AWS CloudTrail trail

★ Key Point

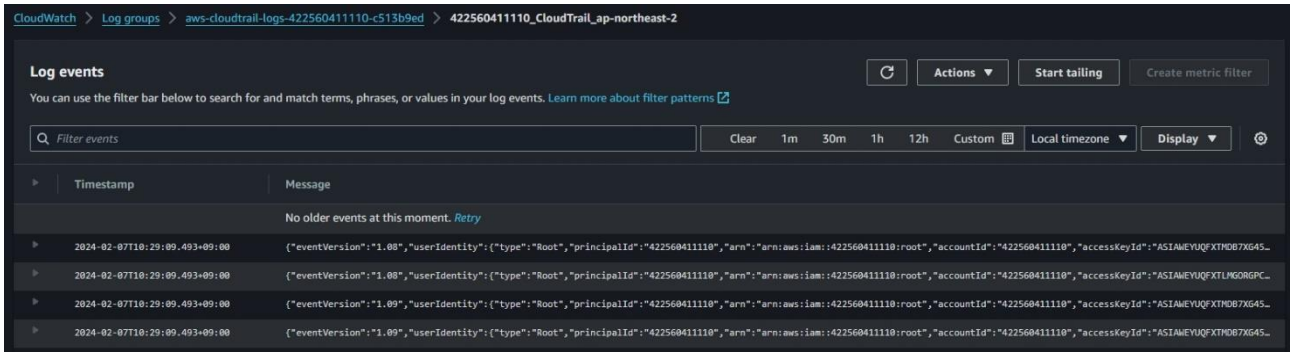
If CloudTrail logs are stored only in an S3 bucket, real-time viewing is not possible. If you need to check it frequently, you can check the log by linking it with CloudWatch.



Source: AWS console website

Figure 21. CloudWatch link settings

Once the link setting is completed, it is added to the CloudWatch log group, and you can set and view the log retention period.



Source: AWS console website

Figure 22. Viewing the AWS CloudWatch log events

■ Closing

So far, we have looked at AWS settings for implementing major ISMS safeguards. For automated risk assessment of cloud assets, you can consider using AWS Config service and AWS Inspector service.

SK Shieldus, Korea's No. 1 security consulting company, provides Information Security Management System (ISMS) certification consulting services for systematic security management of cloud environments based on 20 years of consulting know-how. We have the largest number of professional consultants in the industry and provide optimal improvement plans for each company based on its abundant consulting experience.

SK Shieldus is also leading the way in sharing information security information for public interest. Based on the know-how accumulated by carrying out cloud security projects in 2019, it published a cloud security guide in 2021, and published the second revised edition last year. Through the '2023 Cloud Security Guide', corporate security officials can check how to effectively respond to threats in management areas and meet the standards for changed management areas and compliance. Through this, security managers can apply their own safe security settings and check whether it is possible to respond in advance to threats that may occur in the future.

We hope that you can effectively and systematically respond to ISMS certification in a cloud environment through this security guide and SK Shieldus consulting. More detailed information can be found on the official blog of SK Shieldus.