Technology Reports (Special Articles)

Security Cloud Governance

Special Articles on Use of Public Clouds

Development of a Security Checking Tool For Public Clouds

Innovation Management Department Takuya Nakamura

With the accelerating use of public cloud services around the world, many companies are now using them to run their services and mission-critical system workloads. Public clouds are sometimes used to handle highly sensitive information, making security a very important issue.

This article describes the basic concept of security in public clouds, and discusses the measures and approaches taken by NTT DOCOMO in this regard.

1. Introduction

As of 2021, many companies around the world have started using public cloud[*1] platforms such as Amazon Web Services (AWS)[*2], Microsoft Azure[*3] (hereinafter referred to as "Azure"), and Google Cloud Platform (GCP)[*4] to run their services and mission-critical system workloads[*5]. These platforms are also sometimes used to handle highly sensitive information, making security a very important issue.

However, information incidents including large-scale data breaches and service outages have actually occurred in systems built using public clouds. In one particularly serious case that drew a lot of attention, the personal information of over a hundred million people was leaked from a system built by Capital One in the United States [1]. Many of these incidents would not have occurred had it not been for the use of public clouds. However, these platforms offer many advantages, such as the ability to conduct business at a much faster speed. In 2021, it is no longer tenable for corporate management to choose not to use public cloud platforms for security reasons alone.

[*1] Public clouds: Cloud computing services that anyone can use over the Internet.

[*2] AWS: A cloud computing service provided by Amazon Web Services, Inc.

[*3] Microsoft Azure: A cloud computing service provided by Microsoft Corporation.

[*4] GCP: A cloud computing service provided by Google LLC.

NTT DOCOMO has been using public clouds since around 2009. As of 2021, we have gained extensive experience and know-how of using them to run workloads securely. In this article, we describe the basic concepts of security in public clouds. We also introduce NTT DOCOMO's security countermeasures and some examples of efforts we have made to prevent security incidents, and we present the features and configuration of ScanMonster, a security checking tool that we developed based on these efforts.

2. Cloud Security Concepts

Before public clouds became popular, companies often had to prepare their own data centers and servers. This implementation style is now called "on-premises." The biggest difference between on-premises and public cloud platforms is that the former is implemented with servers that the user is entirely responsible for managing, while in the latter, the user does not even need to know about the existence of the data center. In order to successfully use public clouds built on servers that are not directly visible and cannot be directly managed, it is absolutely essential to understand the basic concept of the shared responsibility model, which is described below (in the case of AWS, see [2]).

2.1 Shared Responsibility Model

In a public cloud, the cloud provider operates, manages, and controls various system components, ranging from the host operating system and virtualization layer to the physical security of the facility where the service is operated. This has the benefit of reducing the operational burden on the user, while leaving the cloud provider in charge of providing the service.

However, no matter how many security measures are implemented by the cloud provider, very dangerous situations can still arise depending on the settings made by the user. It is therefore necessary for cloud providers and their users to establish a clear division of responsibilities and to cooperate in the implementation of security measures. This way of thinking is called the shared responsibility model.

In the shared responsibility model of a public cloud, the responsibilities apportioned to users and cloud providers differ depending on the type of service (**Figure 1**). In the case of so-called Infrastructure as a Service (IaaS)*6 services that provide virtual machines*7, the cloud provider is mainly responsible for managing physical facilities such as data centers, hardware such as physical machines and networks, and the host OS and virtualization layer. On the other hand, the user is responsible for managing the guest OS and the applications running on it. In managed services*8 such as Platform as a Service (PaaS)*9 and Function as a Service (FaaS)*10, the user has a narrower scope of responsibility, and a greater share of the management responsibilities can be left to the cloud provider. By making appropriate use of such services, a company can concentrate its resources on value-added applications and business areas.

2.2 Cloud Provider Evaluation

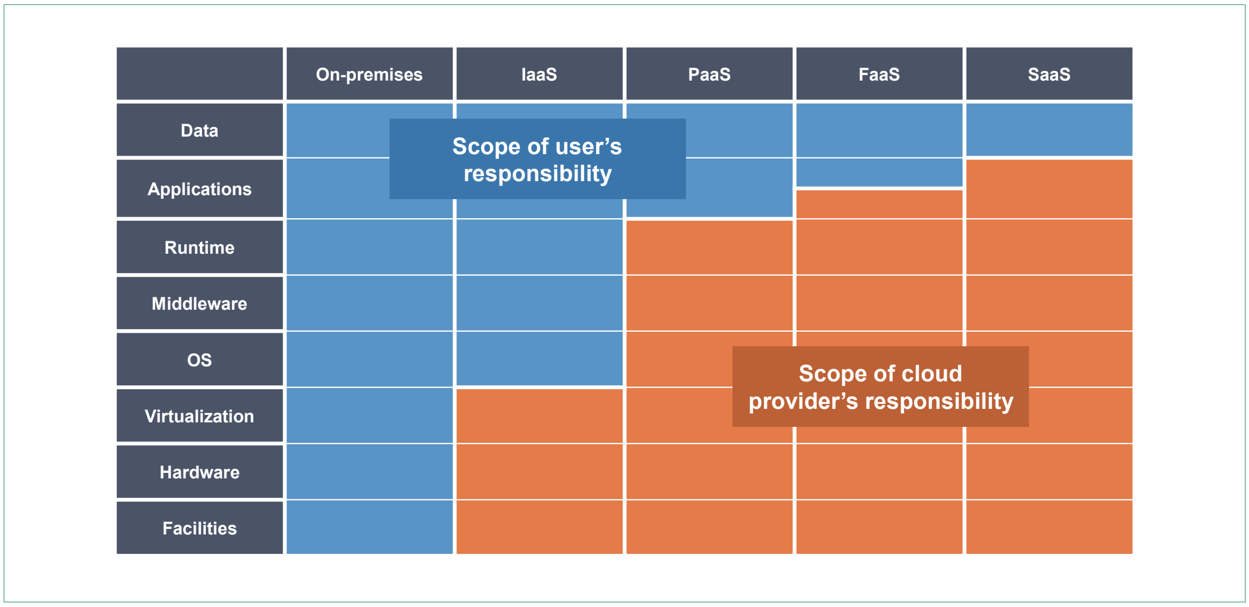
In the abovementioned shared responsibility model, users not only have to share the responsibility

*5 Workload: An indicator of the size of a system's load, such as the CPU utilization rate. In particular, in a public cloud environment, the workload may represent the system itself, including the OS and application code running on the cloud. In this paper, we use the term in this latter sense.

*6 IaaS: A service in which hardware such as servers and networks is rented out virtually to users who use this hardware to install and run their own OS and application software.

*7 Virtual machine: Computers such as servers constructed in a virtual manner by software.

*8 Managed service: Cloud services whose resource provisioning, operation, etc. are mostly the responsibility of the cloud operator. Among cloud computing services, these are referred to as PaaS and SaaS, for example.



	On-premises	IaaS	PaaS	FaaS	SaaS
Data	🟦	🟦	🟦	🟦	🟦
Applications	🟦	🟦	🟦	🟦 🟧	🟧
Runtime	🟦	🟦	🟧	🟧	🟧
Middleware	🟦	🟦	🟧	🟧	🟧
OS	🟦	🟦	🟧	🟧	🟧
Virtualization	🟦	🟧	🟧	🟧	🟧
Hardware	🟦	🟧	🟧	🟧	🟧
Facilities	🟦	🟧	🟧	🟧	🟧

Scope of user's responsibility
Scope of cloud provider's responsibility

Figure 1 Differences in the scope of responsibility for different types of public cloud service

with cloud providers, but conversely they also have to entrust certain aspects of the service to them, and must therefore be able to trust that the cloud providers can fulfill their responsibilities. But is this sharing of responsibilities really appropriate? For example, concerns might be raised about a cloud provider's ability to provide a stable service, or to guarantee security, or whether data uploaded by users to public clouds is immune to illicit internal access. So how is it possible to evaluate the trustworthiness of a cloud provider?

Evaluation methods for public clouds and cloud providers need to draw a broad distinction between functional and non-functional requirements.

With regard to functional requirements, it is essential to perform preliminary checks on the documents, white papers, and Service Level Agreements (SLAs)*11 provided by cloud providers. In particular, items such as service availability and performance are often explicitly provided as numerical values in the documentation, allowing them to be evaluated against specific system requirements.

It is also effective to use certificates issued by public institutions and compliance reports issued by audit firms as important decision-making materials for the evaluation of non-functional requirements. Some of these documents are made available to the public by cloud providers, while others have to be obtained through individual non-disclosure agreements. Many cloud providers have been audited by international organizations, including those listed below, and their certifications and reports are available.

- International Organization for Standardization (ISO)*12 27017: 2015 Certification
- Payment Card Industry Data Security Standard (PCI DSS)*13 Attestation of Compliance (AOC)*14 and Responsibility Summary

*9 PaaS: A service that lends out a platform including an OS and middleware for running applications on the cloud. The user creates and uses application software on the borrowed platform.

*10 FaaS: An event-driven application execution service. Since there is no need to manage resources, users can concentrate on writing code. Services of this sort are generally billed according to the time it takes to execute functions.

*11 SLA: A guarantee of the quality of a provided service.

*12 ISO: A organization that sets international standards in the field of information technology plus all other industrial sectors except electricity and telecommunications.

*13 PCI DSS: A credit card security standard established to protect cardholder details and transaction information.

- Service Organization Controls (SOC)[*15] 2 Report

These reports also help to determine whether or not the cloud provider in question meets the security standards of various industries. For example, in the financial sector, the Center for Financial Industry Information Systems (FISC) has set out security standards, and many cloud providers have published details on how they are complying with these standards.

In recent years, the EU has also been actively passing laws and regulations to protect the privacy of users, such as the General Data Protection Regulation (GDPR). To implement public cloud services that comply with the laws and regulations of each region or country, public cloud providers use separate physical data centers for each region (or country). This makes it possible for them to provide clear indications of data residency[*16] and offer services that are customized to meet the legal compliance requirements of each country/region.

2.3 Measures to be Taken by Users

The measures to be taken by users in public clouds are basically the same as those taken by the users of on-premises systems. For example, they should manage latent vulnerabilities in software and encrypt communications, and when using IaaS services, they should also ensure that security patches are applied to guest operating systems, and set up firewalls to prevent attacks at the network level.

Incidentally, do public clouds have any other advantages apart from the fact that the maintenance and operation of physical data centers and servers is taken care of by the service provider? One of the main factors behind the widespread use of public clouds is their PaaS mode of operation. With PaaS, there is no need for the user to manage the OS, which is necessary with IaaS. Furthermore, in PaaS, and especially FaaS where users only need to their own code, there is no need for users to take responsibility for the management of middleware[*17]. Therefore, the reduced management obligations of the user compared with on-premises (or IaaS) solutions means that the user bears less of the responsibility for implementing security measures. In other words, the use of PaaS and FaaS has the effect of reducing the user's exposure to security risks.

On the other hand, there have been some incidents that could only have happened in cloud services. In the cloud, all infrastructure[*18] is implemented in software. In the past, setting up infrastructure involved entering a server room and disconnecting and reconnecting LAN cables to provide an external network connection, but nowadays this can be done at the push of a button. Although businesses can benefit from this ability to make quick and decisive infrastructure changes from a maintenance terminal with such ease, this also raises major concerns with regard to security.

Cloud providers offer a number of services that are useful for implementing security measures within the user's realm of responsibility. For example, AWS publishes a collection of best practices called the AWS Well Architected Framework[*19]. It is also very important to use tools such as AWS Trusted Advisor and Security Hub to check whether a system is being operated in accordance with best

[*14] AOC: A certificate that indicates a service provider's compliance with the PCI DSS standard.

[*15] SOC: Security standards developed by the American Institute of Certified Public Accountants. Also called System & Organization Controls.

[*16] Data residency: The location where data is stored.

[*17] Middleware: Software providing functions for common use by multiple applications.

[*18] Infrastructure: A generic term for the physical or virtual data centers, servers, networks and other equipment needed to run an application.

[*19] AWS Well Architected Framework: A set of best practices for design and operation published by AWS.

practices in the realm of user responsibility.

3. Security Controls at NTT DOCOMO

This section describes NTT DOCOMO's security control concepts and systems.

3.1 Security Control Systems

Our security control systems for cloud operations are shown in **Figure 2**. In this figure, the Information Security Department is a company-wide organization that creates and manages security policies, and can also examine individual systems and offer advice on whether they meet these security policies.

NTT DOCOMO owns many of the facilities that make up its communications network and provide communications services. It also still operates many other workloads on-premises. A strict security policy is applied to the execution of these workloads to avoid security incidents. However, the use of a public cloud does not make the security policy any less strict. Instead, a general security policy is established for all systems built within the company, regardless of whether or not they use a public cloud. Therefore, when using a public cloud, it is important to understand particular mechanisms such as the shared responsibility model, and to apply security measures according to their characteristics.

3.2 CCoE Roles and Challenges

As mentioned above, specific concepts and measures must be implemented when using a public cloud. For this reason, NTT DOCOMO established

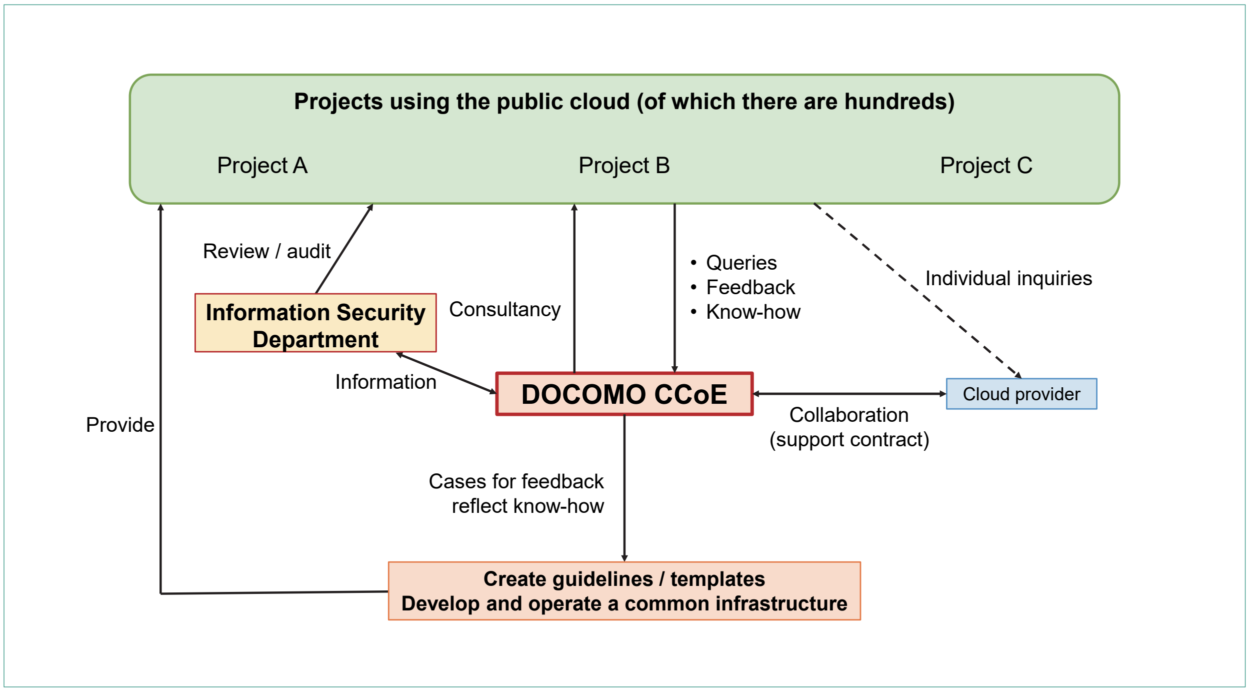

Projects using the public cloud (of which there are hundreds)
Project A
Project B
Project C
Review / audit
Information Security Department
Consultancy
• Queries
• Feedback
• Know-how
Individual inquiries
Information
DOCOMO CCoE
Cloud provider
Provide
Collaboration (support contract)
Cases for feedback reflect know-how
Create guidelines / templates
Develop and operate a common infrastructure

Figure 2 NTT DOCOMO's internal cloud control system

a unit called Cloud Center of Excellence (CCoE), which specializes in supporting the users of cloud computing. This unit shares knowledge with the Information Security Department, provides know-how for each project, and offers consulting on architecture and security.

However, in recent years, the number of systems and projects using the public cloud has grown rapidly, making it difficult for CCoE to keep track of the configuration of every system. Furthermore, although one of the reasons for using the public cloud is to accelerate business, the tightening of control by the Information Security Department and CCoE prevents each project from bringing services to market quickly and adding/modifying functionality with short cycle times. It has therefore become necessary for the members of each project to grasp the business requirements and system configuration by themselves and to make their own judgement of security risks. For this reason, CCoE provides the DOCOMO Cloud Package (a cloud-related knowledge base), and ScanMonster (a security checking tool).

The activities of CCoE are described in more detail elsewhere [3].

4. Visualization and Checking Tools

At the start of each project, the developers first use the DOCOMO Cloud Package to acquire know-how relating to the public cloud in particular, which they can then use to build the system. However, when we conducted interviews relating to each project, many developers said they did not know which know-how to apply, or whether the constructed system would be able to meet policy requirements. To address these issues, CCoE developed ScanMonster, which is a tool that automatically assesses AWS environments.

4.1 ScanMonster Functions

ScanMonster makes it possible to assess an AWS environment in over 70 different ways. Items for assessment are created by referring to the contents of the DOCOMO Cloud Package, the Center for Internet Security (CIS) Benchmarks[*20], the AWS Well Architected Framework, and several other indicators. For example, with the Root Account MFA assessment item, it is possible to check for AWS accounts where Multi-Factor Authentication (MFA)[*21] has not been set up for the root user[*22]. The results of this check can be used to encourage users to set up MFA for the root user if they have not already done so. The ACM Validation Method assessment item checks whether the Domain Name System (DNS)[*23] is used for domain validation when issuing certificates in AWS Certificate Manager[*24]. This is an original item that is based on the contents of the DOCOMO Cloud Package and makes use of NTT DOCOMO's public cloud know-how.

Figure 3 shows a screenshot of ScanMonster in operation. Users can select any of the assessment items and run them at the press of a button. The results are shown as either ○ for success or × for failure, so the user can grasp the assessment results at a glance. It is possible to run multiple assessment items, even all of them, at the same time. It is also possible to run simultaneous assessments by selecting multiple accounts from among

[*20] CIS Benchmark: A security standard developed by CIS in the United States.

[*21] MFA: Multi-factor authentication. An authentication method where a user's identity must be verified with multiple types of evidence (factors).

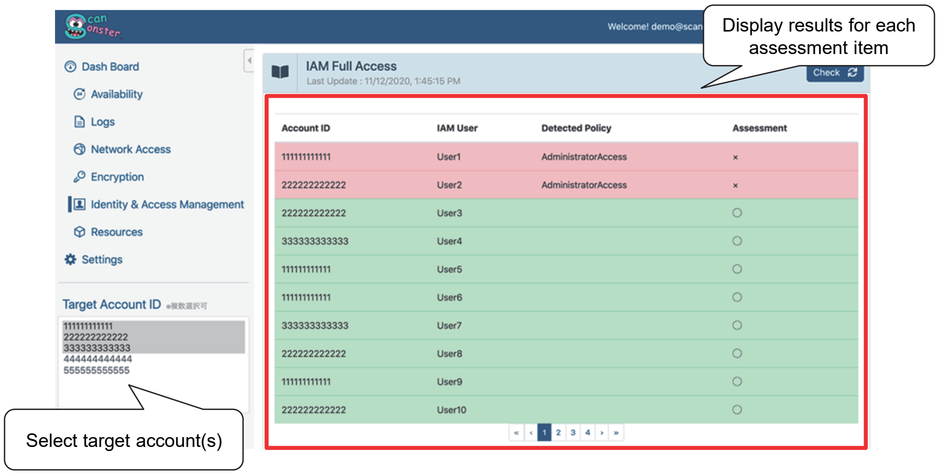
[*22] Root user: A sign-in identity that has complete access to an AWS account. It is considered a best practice to protect this user with strict security by setting up MFA.

[*23] DNS: A mechanism that manages the mapping of domain names and IP addresses on the Internet and provides services for converting between them.

[*24] AWS Certificate Manager: A service that simplifies the issuance and management of SSL/TLS certificates for use with AWS services.

the assessable AWS accounts configured in advance for each user.

For many of these assessment items, tutorials have been prepared to describe the purpose of each item, its pass/fail conditions, and procedure for fixing failed assessments. A screenshot of a tutorial display in ScanMonster is shown in **Figure 4**. These tutorials make it easy for AWS novices to understand assessment results, estimate business risks, and decide whether to take remedial action.

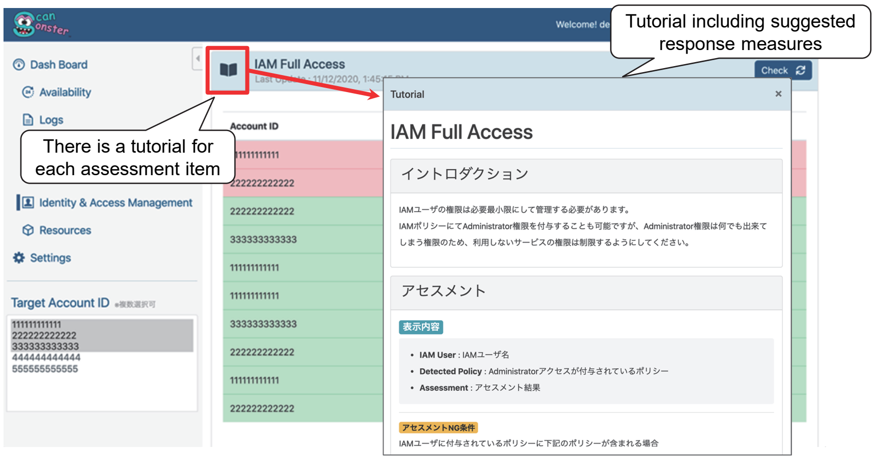


IAM Full Access
Last Update : 11/12/2020, 1:45:15 PM

Account ID	IAM User	Detected Policy	Assessment
111111111111	User1	AdministratorAccess	×
222222222222	User2	AdministratorAccess	×
222222222222	User3		○
333333333333	User4		○
111111111111	User5		○
111111111111	User6		○
333333333333	User7		○
222222222222	User8		○
111111111111	User9		○
222222222222	User10		○

111111111111
222222222222
333333333333
444444444444
555555555555

Figure 3　Screenshot of ScanMonster while running an assessment


can onster
Welcome! de
Dash Board
Availability
Logs
Identity & Access Management
Resources
Settings
Target Account ID ※複数選択可
There is a tutorial for each assessment item
Tutorial including suggested response measures
Check
Tutorial
×

IAM Full Access
Last Update : 11/12/2020, 1:45:15 PM

Account ID
111111111111
222222222222
222222222222
333333333333
111111111111
111111111111
333333333333
222222222222
111111111111
222222222222

111111111111
222222222222
333333333333
444444444444
555555555555

IAM Full Access

イントロダクション

IAMユーザの権限は必要最小限にして管理する必要があります。
IAMポリシーにてAdministrator権限を付与することも可能ですが、Administrator権限は何でも出来てしまう権限のため、利用しないサービスの権限は制限するようにしてください。

アセスメント

表示内容

- **IAM User** : IAMユーザ名
- **Detected Policy** : Administratorアクセスが付与されているポリシー
- **Assessment** : アセスメント結果

アセスメントNG条件

IAMユーザに付与されているポリシーに下記のポリシーが含まれる場合

Figure 4　Screenshot of a tutorial display in ScanMonster

4.2 ScanMonster Configuration

1) Serverless Architecture

As shown in **Figure 5**, ScanMonster is itself built on AWS. Instead of configuring components from IaaS products such as Amazon EC2, it uses services such as AWS Lambda*25, Amazon S3*26, Amazon DynamoDB*27, Amazon Cognito*28, Amazon CloudFront*29 and AWS Web Application Firewall (AWS WAF)*30 to create a serverless architecture.

A serverless architecture has two main advantages.

The first is that, just as the name implies, there is no server and therefore no need for infrastructure management. Since all services are managed services, there is no need to monitor operational status of servers or provision*31 them according to load.

The second is that the operating cost is very low. The only parts that are billed based on the duration of use are AWS WAF, which is used for controlling access to the end-points and to Amazon S3 (which stores the front-end data), and Amazon Cognito, which is used for setting the user management and access permissions. For AWS Lambda and Amazon DynamoDB, since usage fees are only charged when assessments are performed, no fees are charged during periods when assessments are not being performed, even while ScanMonster is still in use, or during periods such as late at night when no one is accessing ScanMonster. The actual monthly cost at NTT DOCOMO ranges from a few tens of yen to a few hundred yen (**Figure 6**).

2) Cross-account Access for Assessment of Multiple AWS Accounts

Simultaneous assessment of multiple AWS accounts is performed with cross-account access by

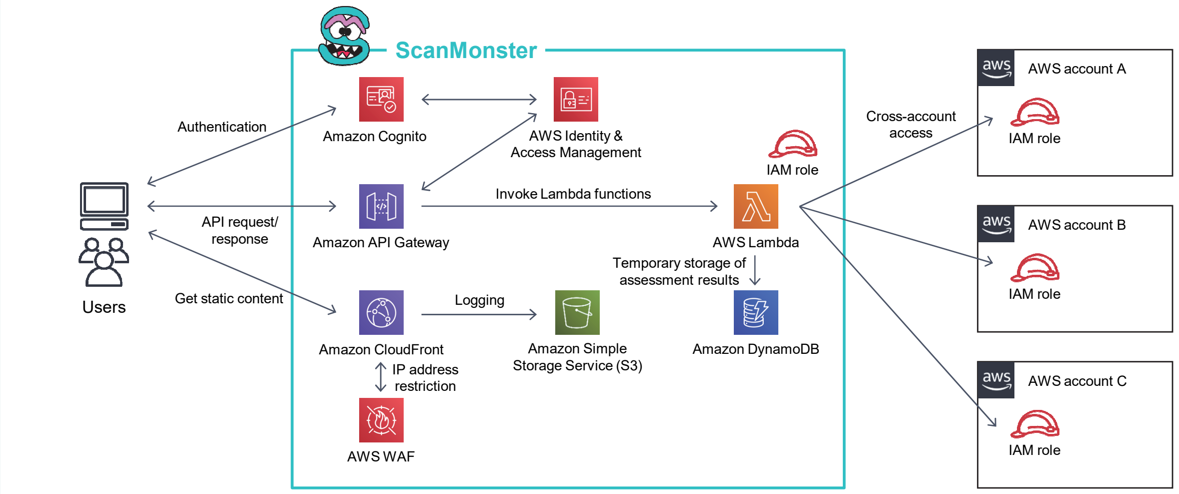


Figure 5 ScanMonster architecture diagram

*25 **AWS Lambda:** A type of FaaS provided by AWS that provides an execution environment for application code so that the user need only register created source code to run the application.

*26 **Amazon S3:** An object storage service provided by AWS. Designed to provide 99.999999999% data durability.

*27 **Amazon DynamoDB:** A NoSQL database service provided by AWS. It is designed to be able to handle large numbers of requests with low latency.

*28 **Amazon Cognito:** A PaaS offering provided by AWS. It provides authentication, authorization, and user management functions for web and mobile applications.

*29 **Amazon CloudFront:** A Content Delivery Network (CDN) service provided by AWS.

*30 **AWS WAF:** A firewall service for web applications provided by AWS.

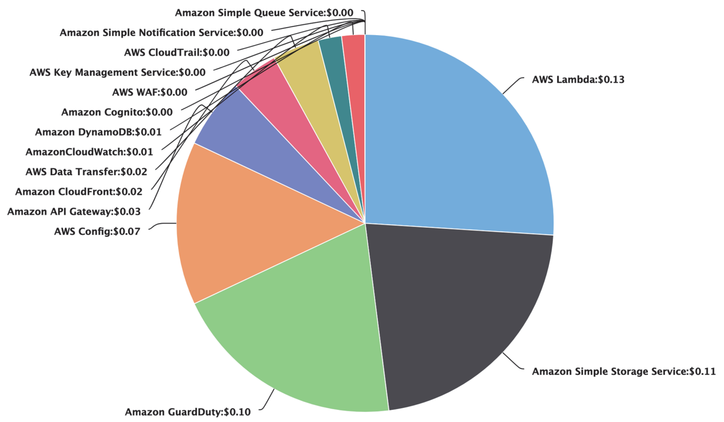


Figure 6 ScanMonster cost performance chart

assuming an Identity and Access Management (IAM) role[*32]. In the AWS account to be assessed, grant access to ScanMonster by setting up an IAM role that trusts the AWS account that deployed ScanMonster. This ensures that assessments are only accepted by AWS accounts that have explicitly granted access. The permissions of the IAM role are restricted to the minimum read permissions needed to perform assessments, so as to prevent unauthorized attacks from the AWS account where ScanMonster is deployed. Furthermore, if Amazon Cognito users are also managed within ScanMonster, it will also be possible to set up AWS accounts that can be accessed by each user.

3) Simple ScanMonster deployment using Infrastructure as Code (IaC)[*33]

All the AWS resources from which ScanMonster is built are written using AWS CloudFormation[*34] templates, allowing it to be deployed instantly. This makes it possible to automatically create a new ScanMonster environment every time testing and quality control is performed during application development. ScanMonster is also a product offered to external customers, which makes it easy for customers to deploy ScanMonster within their own AWS accounts. This allows them to store and use highly confidential security information such as the assessment results of AWS environments without disclosing it to NTT DOCOMO.

5. Conclusion

We have described the basic concepts of cloud security and the efforts that NTT DOCOMO is making with regard to security control. Public cloud technology is still evolving, and the concepts of cloud security and attack methods in the wild are in constant flux. The important thing is that once a system has been created on a public cloud, it is not the end of the story. Security assessments

[*31] Provisioning: The process of securing and configuring resources such as servers and networks to run applications.

[*32] IAM role: One of the identity resources in AWS. It is used to delegate access rights to AWS resources to any authorized user, application or service.

[*33] IaC: The process of describing and managing the configuration of infrastructure such as servers, networks, and storage by means of code statements. It can be used to automate configuration and provisioning tasks.

[*34] AWS CloudFormation: An AWS service offering that implements IaC by providing provisioning and management functions for AWS resources described in a template.

should still be conducted on a daily basis, and the contents of assessments should be updated every day to keep up with the times. To perform updates, it is essential not only to use the services provided by cloud providers themselves, but also to create and operate organizations such as CCoE that are dedicated to promoting cloud use and controlling security in order to keep up with the rapid evolution of public cloud services.

NTT DOCOMO developed ScanMonster as a tool that enables autonomous security assessments of numerous internal projects. By using these tools together with a set of guidelines, we have established a system that allows public cloud environments to be used safely without restricting the speed of business. We are considering expanding ScanMonster in the future to include functions for customizing the details of assessments, linking assessments with guidelines, and providing support for multiple cloud systems including GCP and Azure in addition to AWS. We also aim to make improvements to our internal structures and security policies, such as consolidating the assessment results at the Information Security Department and studying mechanisms for performing assessments on a regular basis.

REFERENCES

[1] Bloomberg: “Capital One Says Breach Hit 100 Million Individuals in U.S.,” Jul. 2019.
https://www.bloomberg.com/news/articles/2019-07-29/capitalone-data-systems-breached-by-seattle-woman-u-s-says

[2] AWS: “Shared Responsibility Model.”
https://aws.amazon.com/compliance/shared-responsibility-model/

[3] H. Moriya, et al.: “NTT DOCOMO’s Use of Public Clouds and Role of CCoE,” NTT DOCOMO Technical Journal, Vol.23, No.1, pp.4–12, Jul. 2021.