# **Amazon Cloud Risk IT Audit**

# 1. Description of the organization and existing operations

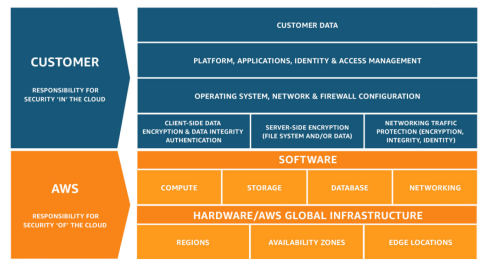
Amazon Web Services is a cloud database platform provided by Amazon. Its main business includes data cloud hosting services and cloud computing services. Because of flexible security configuration model, AWS customers set configuration and costs according to business needs. Therefore, AWS has been a leading brand in the field of cloud services. Even the CIA uses AWS to host data.

Amazon Cloud emphasizes on taking risks with customers and establishes a model of shared responsibility. It stipulates that AWS is responsible for providing the underlying infrastructure hardware facilities and all security configuration control mechanisms; customers choose some suitable security configuration control mechanisms and maintain the security of their cloud database by setting specific configuration parameters.

## 1.1 AWS responsibility sharing model

AWS is responsible for "security of the cloud itself" - AWS protects the infrastructure that runs all AWS cloud services. This basic implementation consists of hardware, software, networks, and devices running AWS cloud services [1]. That is to say, Amazon provides general hardware equipment, corresponding software and network protection.

The customer is responsible for "security within the cloud" - Customer responsibility is determined by the AWS cloud service selected by the customer. It determines the amount of configuration work that the customer must complete when fulfilling safety responsibilities. In other words, customers need to set security configuration parameters and manage data hosted on AWS (encryption / storage / retrieval)



# 2. AWS weakness and potential risk

## 2.1 Internal human factors

Global telecommunications giant Verizon pointed out in a report that nearly a quarter of the data breaches were caused by the operation or active disclosure of insiders. 80% of data breaches are caused by ghosts in enterprises, and hackers and other methods account for only 20%.

### **2.1.1 Inner ghost**

**Weakness**: AWS employees used internal vulnerabilities to leak customer database information.

The relatively low salary of Amazon employees may encourage them to take risks and sell confidential information.

**Potential risk**: Customer information is sold to a third-party company. To make matters worse, competitors may maliciously buy AWS employees, acquire internal company data, and seize customers. For example, according to a report in The Wall Street Journal, Amazon employees reported that they sold confidential customer

information to third-party companies through intermediaries.

### **2.1.2 Management system issues**

**Weakness 1**: The company's supervision of employees' operations is not in place, and no dangerous operations of employees have been detected, such as no restrictions on public access and database encryption. For example, AWS configuration errors caused GoDaddy data to leak[[1]](#endnote-0). According to statistics from the security company Skyhigh Networks, 7% of Amazon S3 buckets are not restricted for public access, and 35% of buckets are not encrypted.

**Potential risk**: For customer companies that use Amazon cloud services, it may lead to passive disclosure of information, or the stored data is lost and cannot be retrieved.

**Weakness 2**: In response to known security vulnerabilities, the management did not pay attention to it and fixed it. Even if the security consultant has submitted a risk report to the management, the management ignores it and refuses to repair it.

**Potential risk**: The vulnerability was acquired by external personnel and directly stolen information from it, which had a great impact on customers and lost the trust of customers, which in turn led to a decline in the number of users and had a very negative impact on the company's reputation.

## 2.2 User configuration

**Weakness 1**: It is difficult to determine which bucket the public should choose for access.

Amazon's cloud initial setup is the default bucket is private. However, customers in the process of configuration, it is often difficult to determine what information should be open to the characteristics of the crowd. At the same time, some configuration may be covered under the protection of the rights of other barrels, when a user access to these barrels, permissions are covered to protect information.

**Weakness 2**: AWS configuration vulnerability

AWS security best practice, the rules change often, cause customer confusion when follow safety practice rules. For example, AWS customers in publicly update or part of the data, the need to set the bucket to "public". However, after the completion of the update tend to forget to follow the current security best practice, rules, set back to "private" state, this change and AWS did not remind. Causes other customers to access buckets that should be in a "private" state.

**Potential risk**:

Many cases show that customers tend to misconfigure their permissions when operating services provided by amazon cloud. The ease with which outsiders can access private databases can lead to massive leaks of corporate user data, causing irreparable damage.[[2]](#endnote-1)

## 2.3 Risk of hacking

**Weakness 1**: In view of frequent user configuration errors in AWS, setting private buckets to be public. Hackers have exploited the vulnerability to periodically scan AWS bucket information, found misconfigured S3 buckets, identified JavaScript files and viewed user information stored in the bucket. Worse, because the permissions of the bucket allows anyone to write code to it, hackers also add Magecart malware to files, and then overwrite existing scripts to monitor, control, or even destroy the website.[[3]](#endnote-2)

**Potential risk**: Hackers steal credit card numbers by capturing a sufficient number of credit card processing sites and inserting codes that steal credit card numbers from e-commerce websites.

**Weakness 2**: Insufficient isolation technology. Cloud services run a large number of virtual machines on a physical server (each used for different customer databases). it saves costs associated with the cloud. However, it also means a higher risk of invasion. Specifically, once a virtual machine is successfully compromised, hackers will invade other virtual machines on the same physical server. Therefore, if a client is implanted with malicious code due to wrong configuration errors, other clients of the same physical server will be invaded even if there is no configuration problem, thereby leaking data.

**Potential risk**: Hackers use memory analysis technology to rent an instance and use it to invade another instance hosted on the same server (this research shows that it is entirely possible to recover the encryption key of the virtual neighbor).[[4]](#endnote-3)

**Weakness 3**: AWS is vulnerable to server-side request forgery [SSRF] attacks

**Potential risk**: SSRF is a server attack that can trick a server into connecting to another server that it does not intend to connect to. In other words, hackers use it to invade the company's internal website from an external website, and then the hacker has the right to execute any command on the internal website, such as obtaining database information. In the case of 2019, Capital One's database firewall hosted on AWS is misconfigured, leading hackers to launch SSRF attacks between March 19 and July 17 and successfully obtain social security numbers as well as bank accountsv.

## 2.4 Poor risk supervision

**Weakness 1**：The elastic block store (EBS) stores all the data for cloud applications, and because these common EBS volumes are for different customers at the same time, coupled with the fact that cloud administrators often do not choose the right configuration, it is easy to inadvertently expose and unencrypt EBS snapshots.

**Potential risk**：If the system administrator sets it up incorrectly, exposing the disk for only a few minutes is enough for the researcher to get a snapshot document and restore the data in the cloud.[[5]](#endnote-4)

**Weakness 2**：High voltage distribution systems do not use fully redundant power supply.

**Potential risk**：In the face of unexpected power cuts, prone to accidents. Redundant power supply is a kind of power supply used in the server. It is composed of two identical power supplies, which are controlled by the chip for load balancing. When one power supply fails, the other power supply can immediately take over its work. In 2012, Amazon data center is located in the eastern United States fail, due to cable fault affecting high voltage distribution system[[6]](#endnote-5).

# 3. AWS current practices, policies and controls

## 3.1 Internal human factors

a.  Trusted Identity Authentication System

Identity authentication is closely related to business scenarios. Different scenarios have different requirements for the strength of identity authentication. This includes identity management, access management, advanced authentication, identity threat analysis, privileged account management, bastion machine, Internet access authentication, and unified website authentication. The most common method to prevent "inner ghosts" is "4A". It solves the problem of "When" through the unified and centralized management of the IT system Account (Account), Authentication (Authentication), Authorization (Authorization) and Audit (Audit)," Where ","What "," Who "," How ".

b. Security situation awareness

Through the use of technology and services such as character portraits, context awareness, threat intelligence, and professional operations to achieve a high hit rate of internal threat discovery, and intelligently cooperate with security protection equipment for real-time control, self-learning character security baseline drives flexible authorization to achieve automation and intelligence After the event, during the event, before the event control.

c. Advanced threat terminal monitoring and response

When discovering data theft or conducting security audits, enterprise security managers urgently need to understand how the attack occurred and which hosts and accounts were compromised. The advanced threat terminal monitoring and response system CTDI is an EDR product for terminal threat detection and response. It is like a high-definition camera for terminal behavior recording. It can aggregate detailed records of kernel state and user state to the server for correlation analysis and advanced Inquire.

## 3.2 Configure vulnerabilities for AWS

a. Preventive control: All publicly accessed buckets are marked orange Through the highlighted Settings, customers can clearly find their own public database, so that customers can more clearly understand their operation and public data, a change in the next operation.

b. Corrective control: Added one key to delete all rule options

A reset button is provided for the administrator to clear the previous Settings, and all custom rules can be overwritten with a single click.

## 3.3 Responding to hacking

a. Amazon has developed tools to help cloud customers stop this type of attack, including the one-click "block public access" option launched last fall. But obviously, it is proved that thousands of domains have not yet locked their infrastructure through the tool, which may have catastrophic consequences. Preventive

b. The use of more powerful isolation technology makes it impossible for hackers to invade other virtual machines through the virtual machines on the same physical server, causing data leakage of other customers. preventive

c. Other Amazon competitors have built-in protection measures for SSRF in their products (including Google since 2013 and Microsoft since 2017), but AWS has not established similar protection measures; Capital One said in July , It has fixed the so-called "configuration vulnerability" preventive / corrective

## 3.4 AWS risk regulation

a. Preventive control: The EBS snapshot is stored on S3, not in its own bucket, and cannot be accessed directly, but only through the EC2 API, so configuring access control on the EC2 API can prevent this

b. Preventive control: In the case of power cuts, in order to protect the data storage, the system will automatically turn to read-only mode, until the power is restored to start the available area, and then resumed as soon as possible to a consistent state, and returns to the mode, data storage, speaking, reading and writing that enable variable EBS call success. But in this case, the protection didn't work.

# 4. The proposed control mechanism

### **4.1.1 For inner ghost**

a. Strengthen safe operation(preventive)

Enterprises should strengthen the whole process security guarantee before, during, and after the event, and create a safe operation system that covers the entire life

cycle of prevention, detection, response, and visibility.

b. Sorting out data security (detective)

Enterprises should strengthen the classification and governance of data management at the beginning of data production, including the perception, risk identification and classification of data, and clearly identify which are confidential data, sensitive data, and ordinary data.

c. Implementation of the solution (corrective)

In the process of data storage, transmission and use, advanced data protection technologies, such as encryption and desensitization technologies, should be fully applied, and confidential data needs continuous protection.

### **4.1.2 Measures to prevent internal employees from operating errors**

a. Regularly review the operation steps of employees, and punish employees with irregular operations. (preventive)

b. Add a monitoring function module to the employee's business operating system. When an error occurs during business operation, the monitoring function module will promptly remind. (detective)

c. If the employee's operation has been wrong and there may be a security threat to customer information leakage, you need to inform the customer in time, and immediately conduct security monitoring or use the key to prevent the customer's data from being leaked. (corrective)

### **4.2 for AWS configuration vulnerability**

a. Increase Access control permissions

If you want to change important access rights, it should be controlled by more than one person, and the administrator needs to change the rights of more than one person to review. (preventive)

b. Increase the time access mechanism

When the permission is changed, you can set up a mechanism to automatically delete the rules, so as not to forget to close the previously established rules after the rule is added. When the set time for automatically stopping the database access is reached, the database access permission will be automatically closed and the rules will be automatically deleted. (corrective)

### **4.3 Responding to hacking**

a. Monitor the configuration of the customer's bucket and promptly warn: by creating safe defaults (instead of keeping system access rights open, or easily guessed by default), or even actively scanning exposure and checking with customers . (detective)

b. The provider carefully checks the security of cloud services and deploys more powerful isolation technologies in the public cloud: keeping each of these co-located virtual machines (or "instances") isolated. (preventive)

c. Built-in protection measures against SSRF. (preventive / corrective)

### 4.4 For the weak supervision of AWS risks management

a. When the system administrator is configuring EBS, configure the permissions of each account and the access rights of the EBS snapshot. (preventive)

b. Full redundant power supply is recommended for high voltage distribution systems as well as for all operational examples and storage and should be tested and audited periodically. (detective/corrective)

# 5．Contingency plan

|  |  |  |
| --- | --- | --- |
| Risk | Responses | Responsible person |
| Internal personnel make mistakes, set private library as public library | 1. Change the settings and back to the private bucket; 2. Notify customers to check account status; 3. Notify the publicist to issue a statement | Emergency Commander, External communication, Business executives |
| Inside Ghost Selling User Information | 1. Alarm 2. Notify customers to check account status 3. Inform public relations personnel to issue a statement 4. Smart protection equipment cooperates intelligently for real-time control 5. Enterprise security managers urgently need to understand how attacks occur and which hosts and accounts are compromised. | IT team leader, Emergency Commander, External communication, Enterprise Security Manager, law enforcement |
| Configuration error | 1. Change the settings, change back to the private bucket or freeze all buckets, and prohibit access; 2. Notify customers to check account status 3. Inform public relations personnel to issue a statement 4. Train customers and set up and configure correctly | Emergency Commander, External communication, Business executives, IT team leader |
| Power outage risk | 1. Start the backup power supply or replace the damaged power supply with a fully redundant power supply 2. Notify maintenance personnel to carry out emergency repairs 3. View data damage. If there is damage, notify the customer | IT team leader, Emergency Commander, Chief of Logistics |
| Hacking | 1. Alarm 2. The IT team looks at the scope of the data breach and fixes the vulnerability 3. Notify customers to check account status 4. Inform public relations personnel to issue a statement | IT team leader, Emergency Commander, External communication, Corporate Security Manager, law enforcement |

**6. Advantages and disadvantages of the shared responsibility model**

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| For Amazon:  1. When customers have data leakage due to their own configuration problems, they do not need to take responsibility (avoid risks); 2. Focus on the platform itself, specializing in security issues; 3. Reduce operating costs, reduce the huge cost of data management and maintenance 4. Quickly provide service plans: AWS provides universal platform services, so it can provide services to customers within seconds (other companies need a few weeks to investigate customer business and provide customized service plans) | For Amazon:  1. Frequent security incidents affect the reputation: because customers are not security experts, they are prone to data leakage incidents caused by customers' own configuration errors; 2. Increase the risk of security vulnerabilities: Hackers invade the AWS server of one of the customers and use the script to infect the databases of other customers in the same network to obtain database information |
| For Customers:  1. Only need to pay for the use of the platform, no data management and maintenance costs, saving money; 2. Greater control authority: Whether it is the protection of applications and content, or the protection of platforms and networks, it is up to the customer to decide 3. Provide organizations with the fine control required: customers optimize their security configuration based on their business characteristics and needs, and strike a balance between security and cloud efficiency (excessive security affects cloud data management and maintenance efficiency) | For Customers:  1. Since they do not have excellent security experts or sufficient risk awareness, they incorrectly configure AWS server parameters and set private storage buckets to public, thereby exposing database data; 2. Move the data of the local server directly to the cloud without data processing such as encryption and setting of access rights, resulting in the disclosure of user's plaintext information 3. Need to train company employees to manage and maintain data in AWS servers 4. Problems with AWS physical servers (damage due to power outage, etc.) lead to inability to access AWS cloud database data, and the company's business is stalled |

# 7. Conclusion

Amazon, as the world's largest cloud service company, occupies 50% of the market, and its data leakage has a huge impact. Therefore, this paper analyzes the data leakage of Amazon Cloud Service, finds its current security vulnerabilities and risks, and proposes improvement plans and disaster response plans for current security measures. In addition, the responsibility sharing model has certain drawbacks. It is recommended that AWS strengthen the security construction of its own system, provide safe and quality services to each customer, and improve the details of the responsibility sharing model.

# Reference

1. <https://www.sohu.com/a/246388779_465914> [↑](#endnote-ref-0)
2. <https://www.wosign.com/Info/2017-1226-01.htm> [↑](#endnote-ref-1)
3. <https://www.wired.com/story/magecart-amazon-cloud-hacks/> [↑](#endnote-ref-2)
4. https://www.bankinfosecurity.com /crypto-keys-stolen-from-amazon-cloud-a-8581 [↑](#endnote-ref-3)
5. <https://baijiahao.baidu.com/s?id=1641437143875360649&wfr=spider&for=pc> [↑](#endnote-ref-4)
6. <https://www.csdn.net/article/2012-06-19/2806750> [↑](#endnote-ref-5)