



Security Services





Foreword

- This lesson covers the concepts and usage of security services on Huawei Cloud, including IAM, DEW, and CTS. It will cover data security, access security, and audits. We will also cover how to systematically design security cloud services.



Objectives

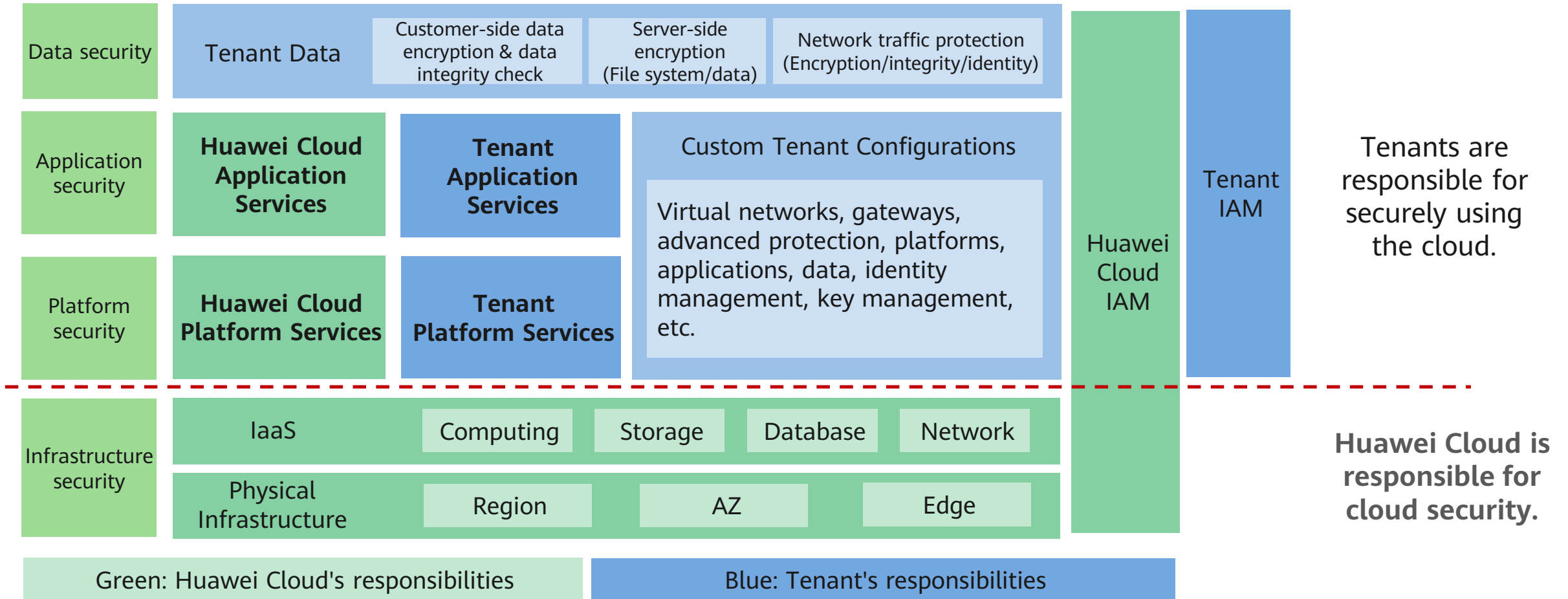
- Upon completion of this lesson, you will understand:
 - The Huawei Cloud shared responsibility model
 - Huawei Cloud security and compliance certifications
 - How to systematically design security services



Contents

- 1. The Shared Responsibility Model for Security**
2. Huawei Cloud Security Certifications
3. Systematic Security Designs

Huawei Cloud Shared Responsibility Model





Contents

1. Shared Responsibility Model for Security
- 2. Huawei Cloud Security Certifications**
3. Systematic Security Designs

Huawei Cloud Security Certifications

ISO 27001:2013

DJCP MLPS

ISO 27017:2015

SOC audit

Singapore MTCS Level 3

PCI DSS

ISO 20000-1:2011

CSA STAR Gold

ISO 27018:2014

TRUCS Gold O&M Assessment

ISO 22301:2012

ITSS Cloud Computing Service Capability
Evaluation by MIIT

Trusted Cloud Service (TRUCS)

Network Security Assessment by CAC

Certification for the Capability of Protecting Cloud
Service User Data

CC EAL3+



Contents

1. The Shared Responsibility Model for Security

2. Huawei Cloud Security Certifications

3. Systematic Security Designs

Access Control at the Cloud Service Layer - IAM

Access Security at the Application Layer - DEW

Audit and Tracing - CTS

Systematic Security Design

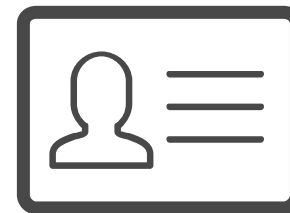
Network security



Compliance standards



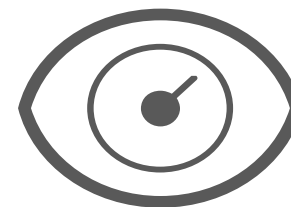
Access control



Data security



Audit and tracking



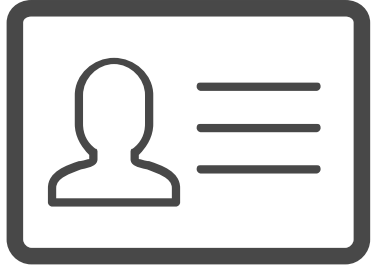
Physical infrastructure security



Event response



IAM Features



Identity and Access
Management
(IAM)


- Major functions:
 - Identity authentication
 - Access management
- Refined permissions management
- Huawei Cloud service authorization
- Identity federation with third-party identity providers or enterprise authentication systems

Identity Authentication Method 1

IAM User Login

Tenant name or HUAWEI CLOUD account name

IAM user name or email address

IAM user password 

Log In

[Forgot Password](#) ☐ Remember me


[Use Another Account: HUAWEI ID | Federated User](#)

- Open the Huawei Cloud console login page.
- Use the IAM username and password to log in.
- Perform fine-grained permissions management on the IAM console.

Identity Authentication Method 2


Use an access key (AK/SK) to verify your identity.
Each IAM user can create two pairs of access keys.






Access Keys

 Access keys can be downloaded only once after being generated. Keep them secure, change them periodically, and **do not share them with anyone**.

Create Access Key

Access keys available for creation: 1

Enter an access key ID. 

| Access Key ID  | Description  | Status  | Created  | Operation |
|---|---|---|---|---|
| R3T38EL2RD5ET5GT9E2R | Demo |  Enabled | Nov 23, 2022 14:15:13 G... | Modify Disable Delete |

An AK contains 20 characters, and an SK contains 40 characters.
An AK/SK pair is used only for API access.
Example command in hcloud →

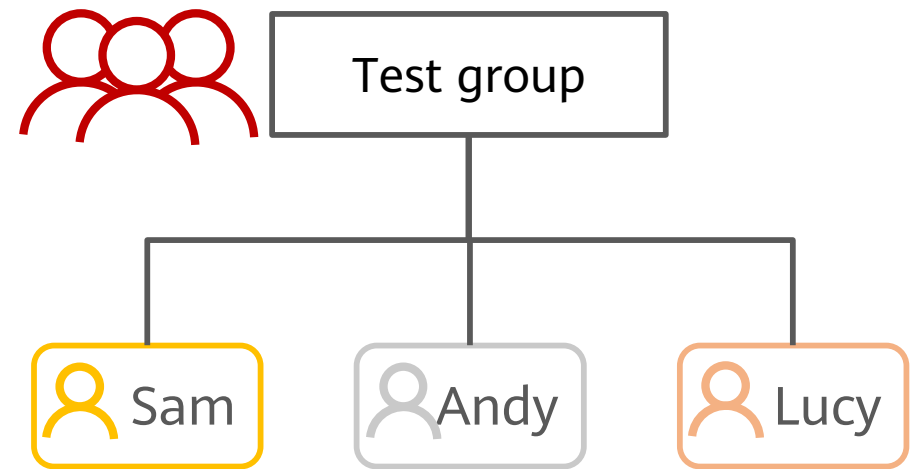
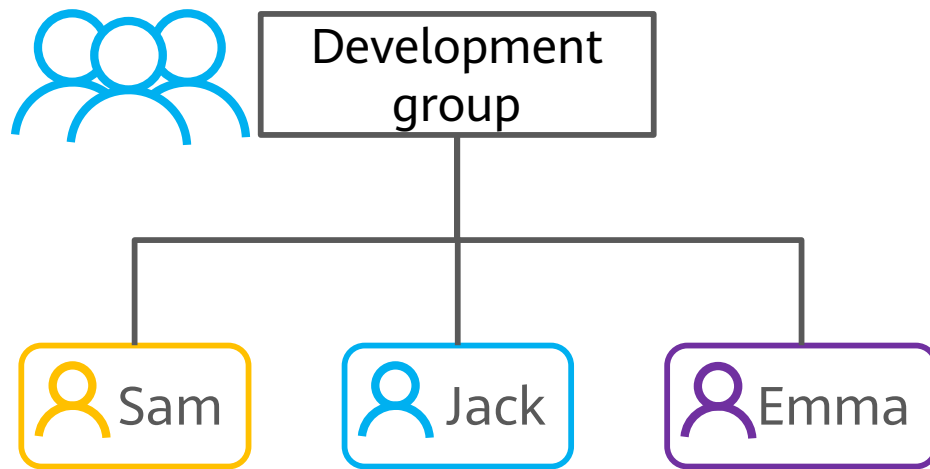
```
D:\>hcloud configure init
Initialization will overwrite the original configuration. Continue? (y/N): y
Starting initialization. 'Secret Access Key' is anonymized. To obtain the parameter,
see 'https://support.huaweicloud.com/usermanual-hcli/hcli_09.html'.
Access Key ID [required]: 
Secret Access Key [required]: 
Region Name: cn-east-3

*****
*****                               *****
*****      Initialization successful      *****
*****                               *****
*****

D:\>
```

IAM User Groups

- An IAM user group is a collection of IAM users.
- An IAM user can belong to different IAM user groups.
- User groups make it easier to manage permissions for users.



IAM Permissions

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:bucket:ListBucket",
        "obs:bucket:Get*"
      ],
      "Resource": [
        "obs:*:*:bucket:*"
      ],
      "Condition": {
        "StringEndWithIfExists": {
          "g:UserName":
            ["specialCharacter"]
        },
        "Bool": {"g:MFAPresent":
            ["true"]}
      }
    }
  ]
}
```

- ❑ IAM permissions are defined in JSON documents.
- ❑ JSON documents are encapsulated into policies for repeated use.

IAM Policies

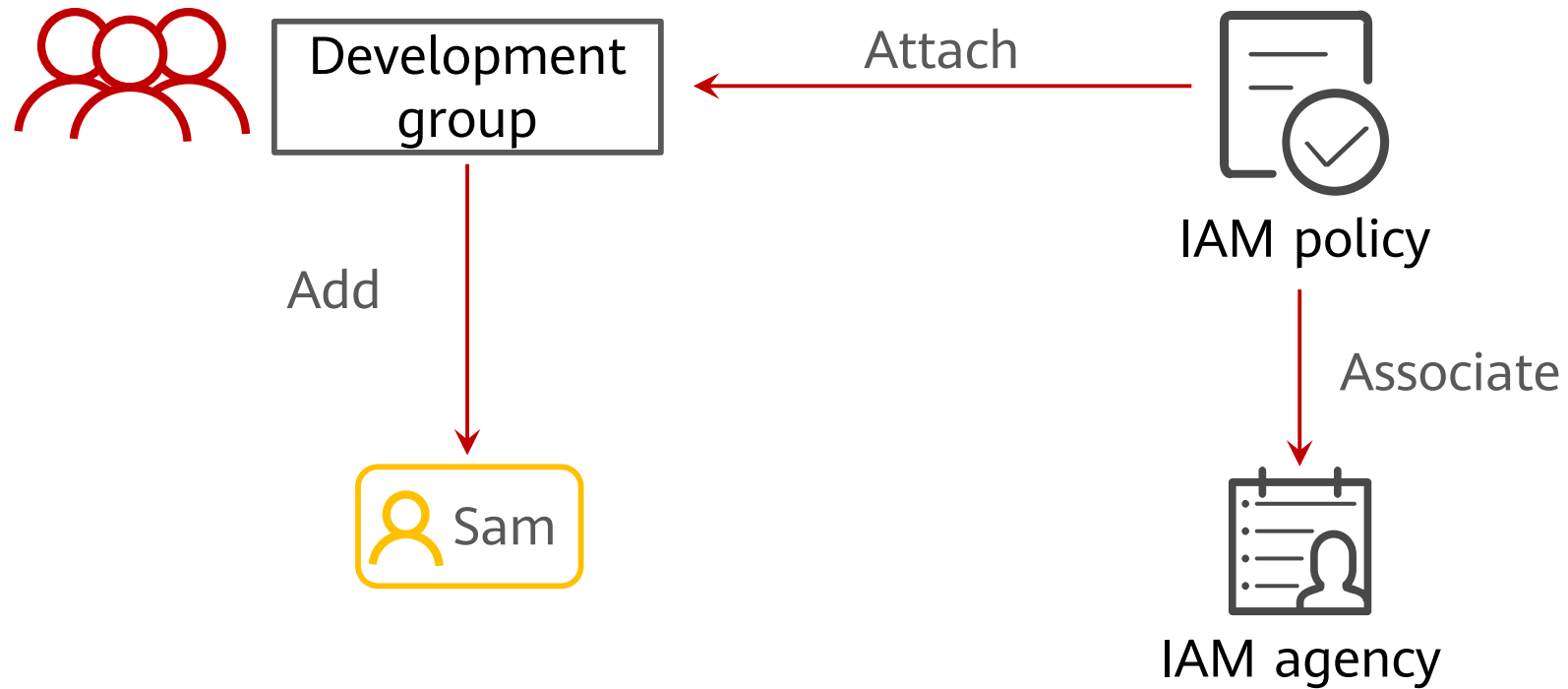
```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:bucket:ListBucket",
        "obs:bucket:Get*"
      ],
      "Resource": [
        "obs:*:*:bucket:*"
      ],
      "Condition": {
        "StringEndsWithIfExists": {
          "g:UserName":
            ["specialCharacter"]
        },
        "Bool": {"g:MFAPresent":
            ["true"]}
        }
      }
    ]
  ]
}
```



IAM policies

- System policies
 - Maintained by Huawei Cloud
- Custom policies
 - Maintained by users

IAM Policy Attachment



IAM Agencies



IAM agencies

- Agencies do not have static credentials.
- Agencies get permissions through policy attachment.
- Agencies enable you to delegate permissions to:
 - Huawei Cloud services
 - Other Huawei Cloud accounts
 - Third-party identity providers

Enabling Applications to Access Huawei Cloud

- To enable Python applications running on an ECS to access data in OBS, how would you obtain access credentials?
 - Create an IAM user and grant OBS access permissions to the user. Then store the AK/SK of the user on the ECS.
 - Create an agency for the ECS and grant the OBS access permissions to the agency. Then associate the agency with the ECS. ✓



Creating an IAM Agency for ECS

On the **Agencies** page, grant the agency permissions of calling APIs to access OBS.

The screenshot displays the Huawei Cloud IAM console interface. On the left sidebar, the 'Agencies' menu item is highlighted. The main content area shows the configuration for a 'Demo ECS Agency'. The 'Basic Information' tab is selected, and the following fields are visible:

- Agency Name:** Demo ECS Agency
- Agency Type:** Cloud service
- Cloud Service:** Elastic Cloud Server (ECS) and Bare Metal Serv...
- Validity Period:** Unlimited
- Description:** Enter a brief description. (0/255 characters)

At the bottom of the form, there are 'OK' and 'Cancel' buttons.

Associating the Created Agency with the ECS

Associate the agency with an ECS so that applications on the ECS can get the permissions granted to the agency.

1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

ECS Name: ☐ Allow duplicate name
If you are creating multiple ECSs at the same time, automatic naming and customizable naming are available for you to select. ?

Login Mode:
The private key will be required for logging in to the ECS and for reinstalling or changing the OS. Keep it secure.

Key Pair: ?

Cloud Backup and Recovery: ?
CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, you are advised to use CBR.

Cloud Eye: ☐ Enable Detailed Monitoring Free ? ! 1-minute fine-grained monitoring has not been enabled. Only the metrics under basic

ECS Group (Optional): ?

Advanced Options: ☒ Configure now

User Data: [Learn how to inject user data.](#)
 0/32,768

Tag:
It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View Predefined Tags](#) C
You can add 10 more tags.

Agency: ?
CPU options: ?

Select the ECS agency.

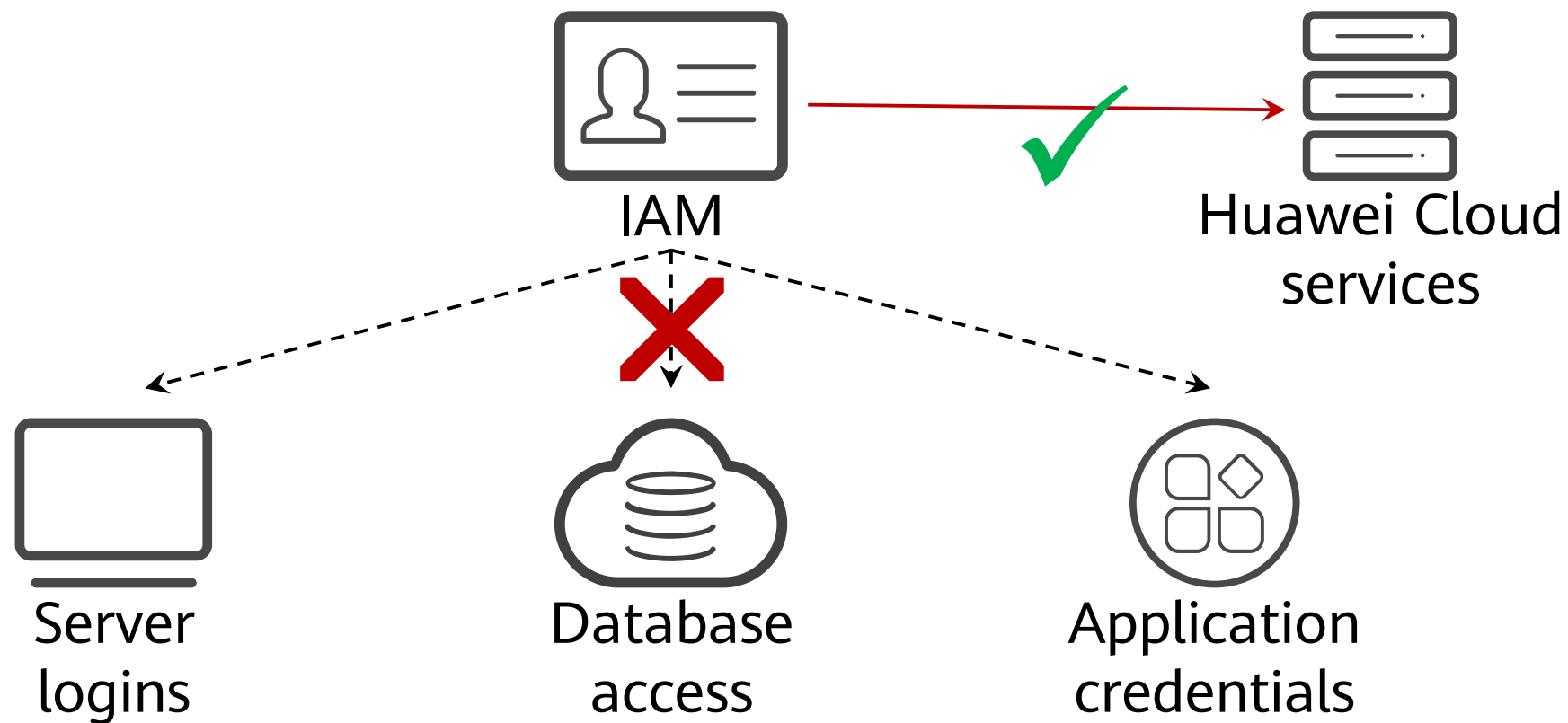
python

Obtain agency permissions to access OBS



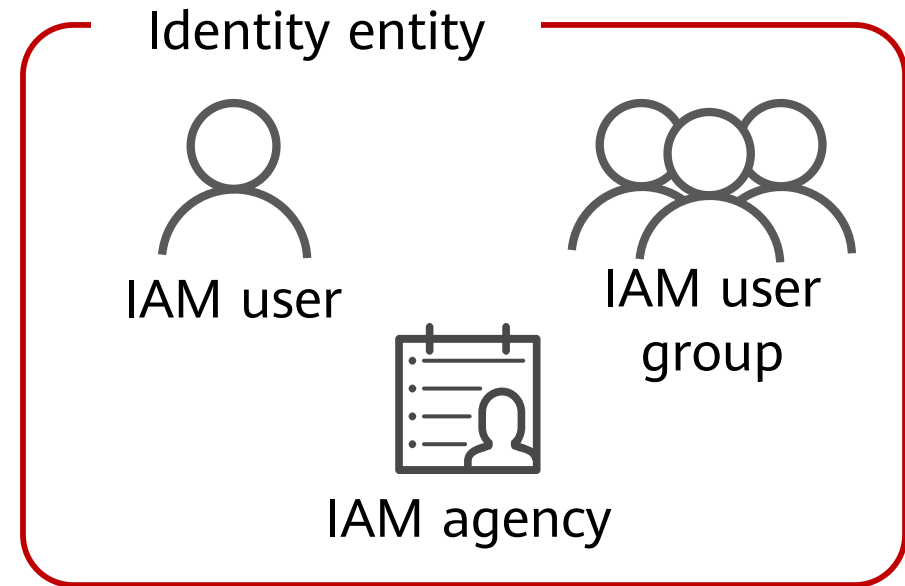
Object Storage Service (OBS)

Access Control Only for Huawei Cloud Services



IAM Summary

- Identity authentication
 - Console
 - Username and password
 - Programmatic access
 - AK/SK
- Access management
 - Policies defined by JSON documents





Contents

1. Shared Responsibility Model for Security

2. Huawei Cloud Security Certifications

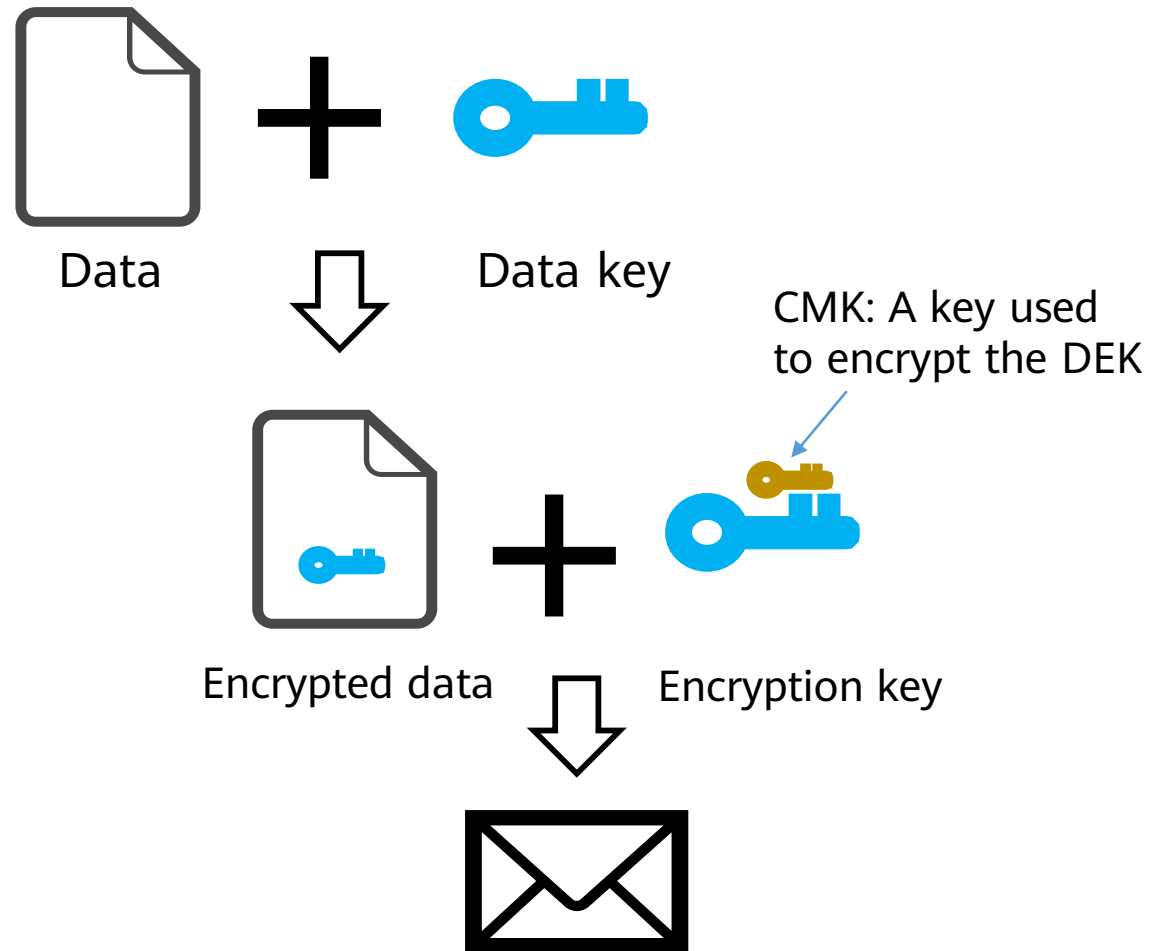
3. Systematic Security Designs

Access Control at the Cloud Service Layer - IAM

Access Security at the Application Layer - DEW

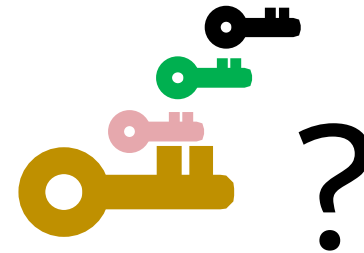
Audit and Tracing - CTS

Data Encryption



Envelope encryption

- There are data keys and CMKs.
- The ciphertext and data keys are stored together for easy management.
- The impact of losing data keys is controllable.



How do you securely store a CMK?

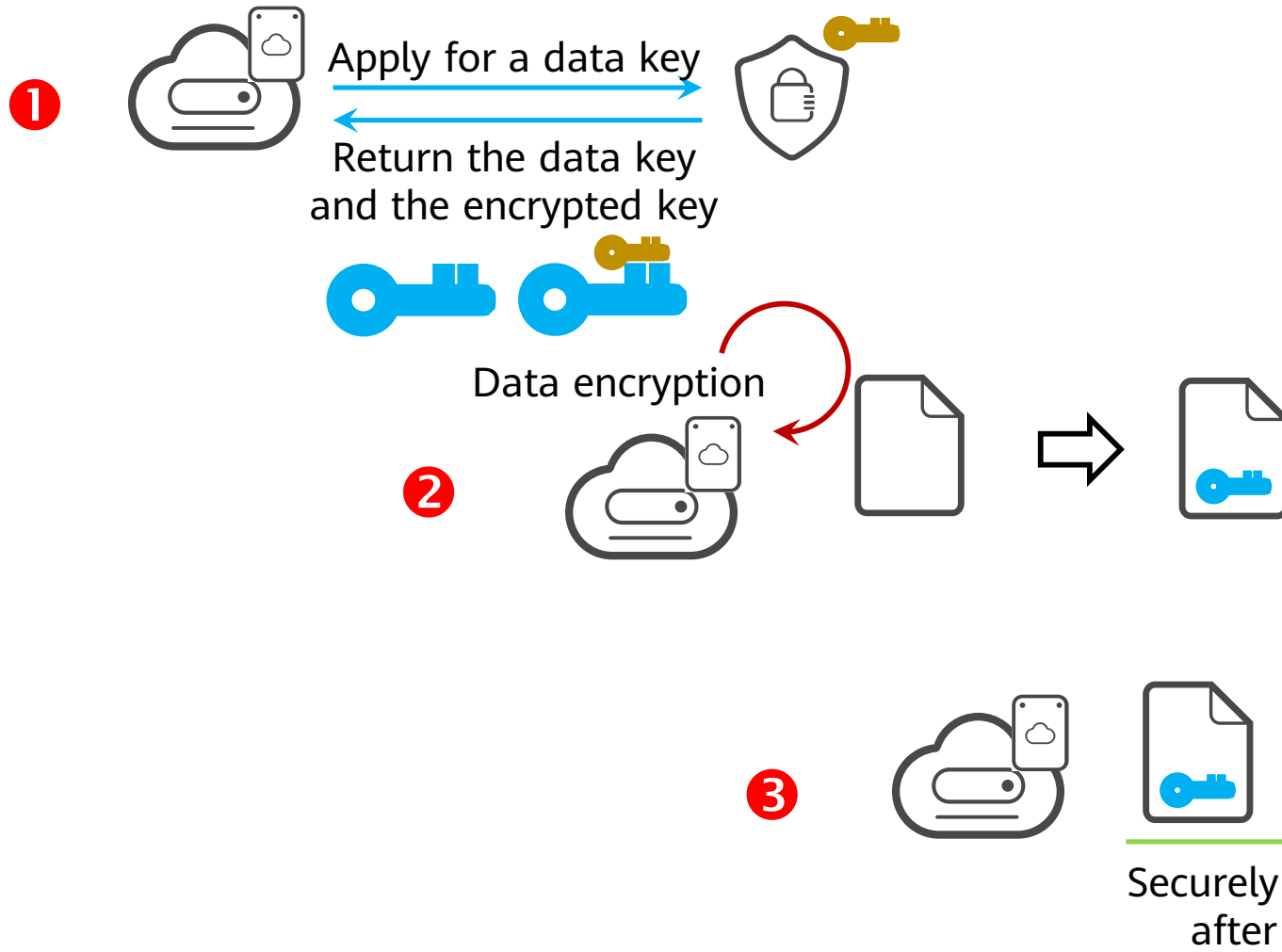
Using DEW to Manage Secrets in Applications



DEW

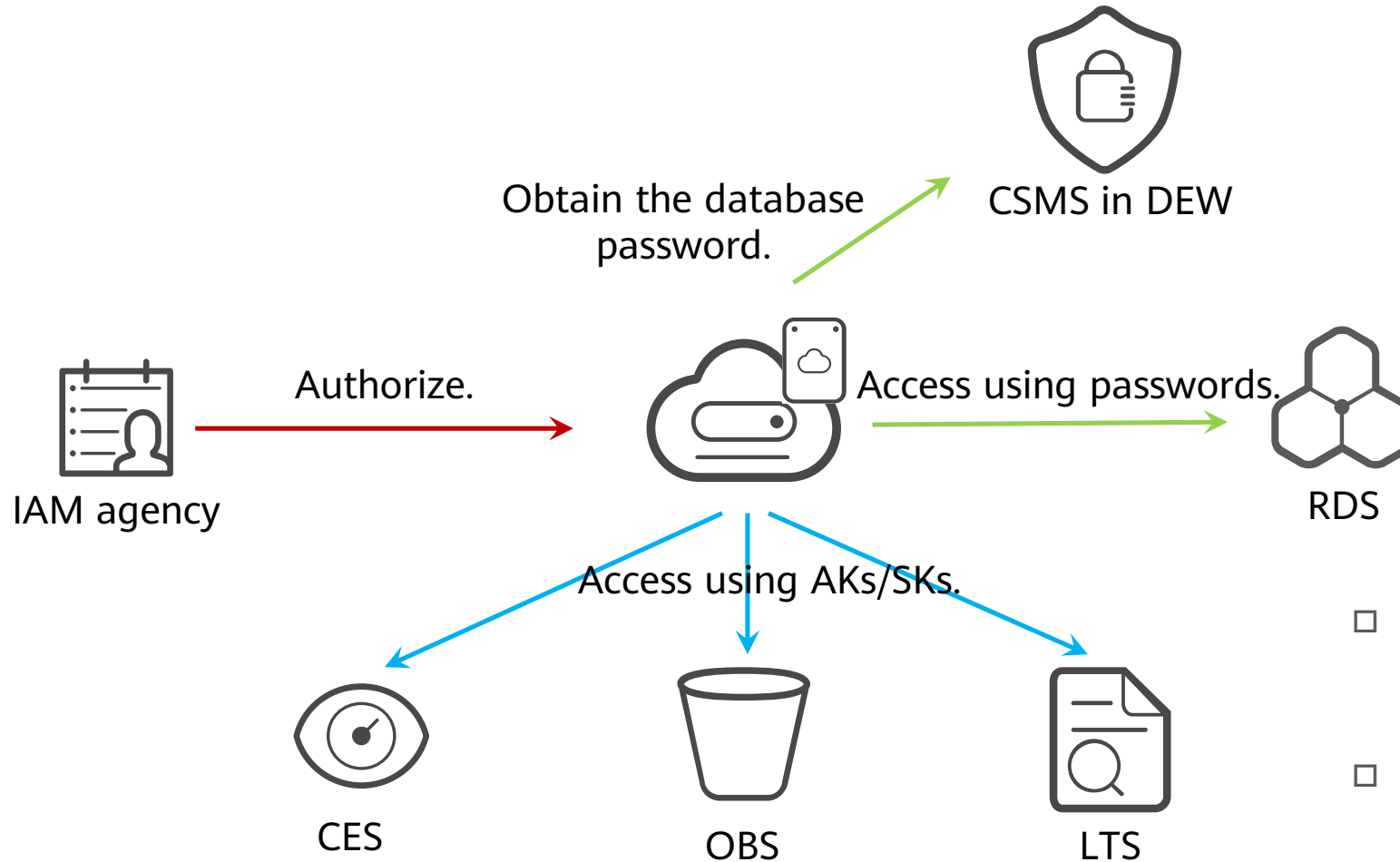
- Secret management
- Database and server passwords can be stored in a centralized manner.
 - You no longer need to write them in your code or configurations.
- Seamless access with IAM agencies

Using KMS for Data Encryption and Decryption



- CMKs never leave DEW.
- DEW allows you to:
 - ✓ Create a data key.
 - ✓ Encrypt a data key.
 - ✓ Decrypt a data key.

Using CSMS to Create a Keyless Architecture



- The entire system **does not record any secrets.**
- IAM agencies are used as the authorization core.
- IAM can also be used for access control.



Contents

1. Shared Responsibility Model for Security

2. Huawei Cloud Security Certifications

3. Systematic Security Designs

Access Control at the Cloud Service Layer - IAM

Access Security at the Application Layer - DEW

Audit and Tracing - CTS

Enabling CTS

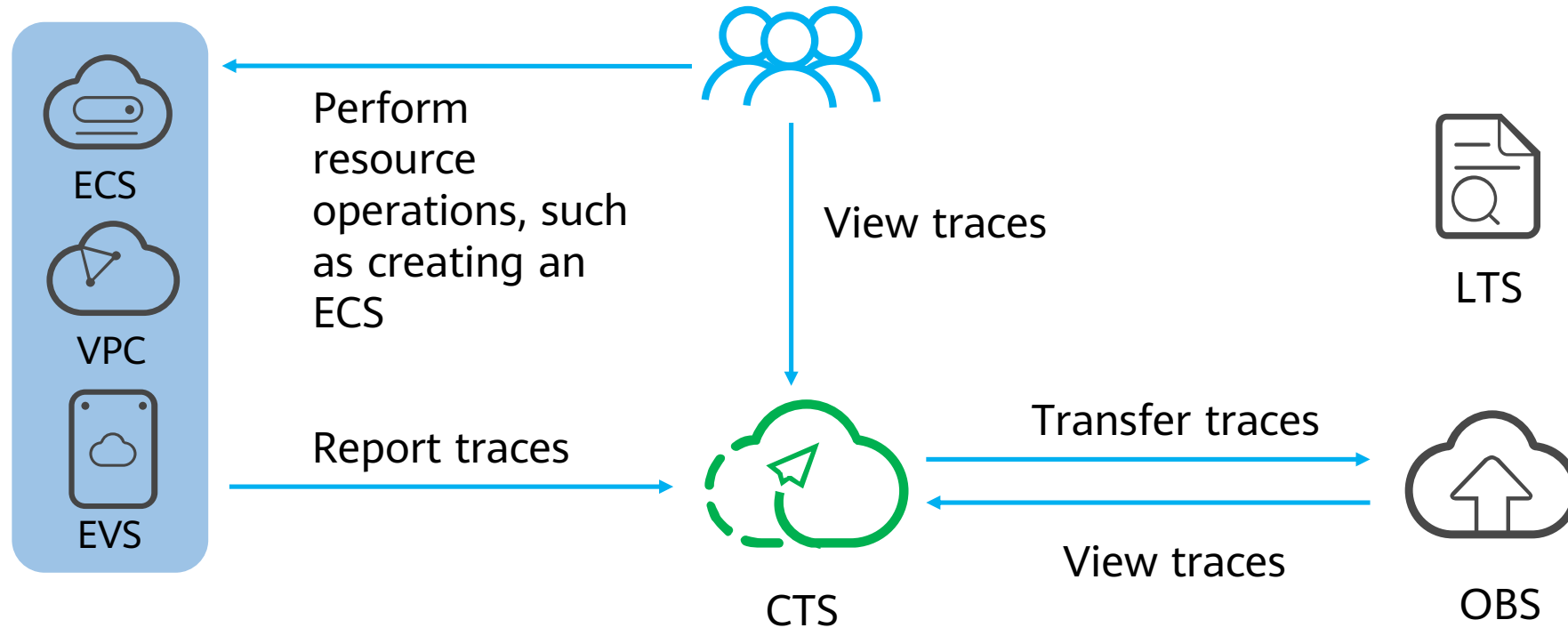


Cloud Trace Service (CTS)

- Manage operation logs on Huawei Cloud resources.
- Filter and query records from the last seven days.
- Analyze real-time LTS operation logs.
- Store logs in OBS for as long as needed.
- CTS itself is free of charge.
 - Charges apply if you transfer traces to OBS, LTS, or DEW.

Cloud Trace Service (CTS)

- CTS records requests and results of operations (API calls) on cloud service resources for you to query, audit, and backtrack operations.





Summary

In this lesson, we covered:

- The Huawei Cloud shared responsibility model
- Huawei Cloud security certifications
- Systematic design of security services

Quiz

Suppose you find that a server was deleted. Which of the following services can help you determine which Identity and Access Management (IAM) user deleted the server?

- A. Cloud Trace Service (CTS)
- B. Cloud Eye
- C. Data Encryption Workshop (DEW)
- D. Identity and Access Management (IAM)



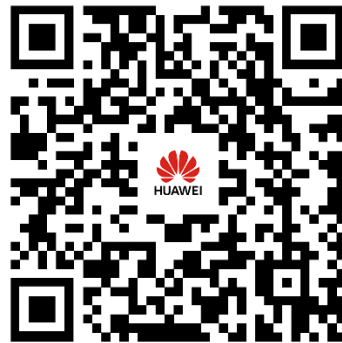
Acronyms and Abbreviations

- IAM: Identity and Access Management
- CTS: Cloud Trace Service
- DEW: Data Encryption Workshop
- KMS: Key Management Service



Recommendations

- Huawei Cloud websites
 - Huawei Cloud: <https://www.huaweicloud.com/intl/en-us/>
 - Huawei Cloud Developer Institute: <https://edu.huaweicloud.com/intl/en-us/>



Huawei Cloud
Developer Institute

Thank You.

Copyright © 2024 Huawei Technologies Co., Ltd. All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



www.huaweicloud.com