HUAWEI

Security Services

HUAWEI CLOUD
EVERYTHING AS A SERVICE

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.

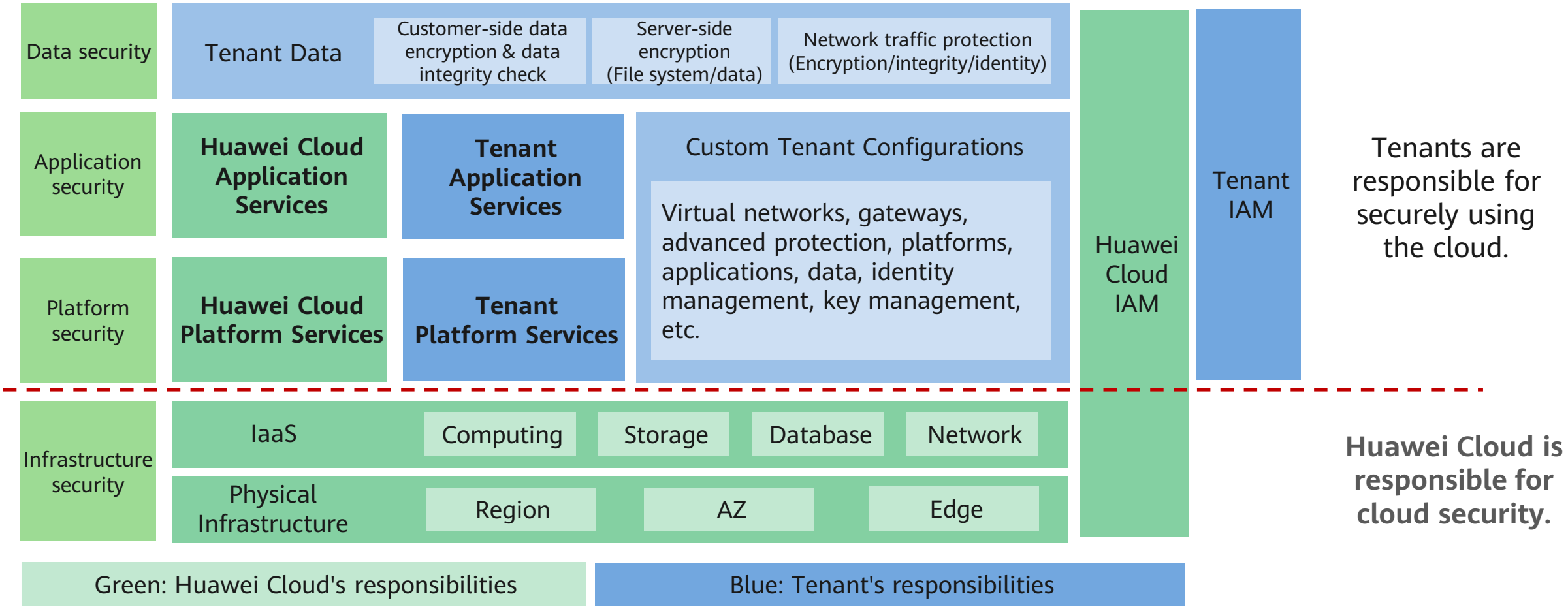
Objectives

- 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

HUAWEI

Huawei Cloud Shared Responsibility Model



HUAWEI

Contents

HUAWEI

Huawei Cloud Security Certifications

ISO 27001:2013

ISO 27017:2015

Singapore MTCS Level 3

ISO 20000-1:2011

ISO 27018:2014

ISO 22301:2012

Trusted Cloud Service (TRUCS)

Certification for the Capability of Protecting Cloud Service User Data

DJCP MLPS

SOC audit

PCI DSS

CSA STAR Gold

TRUCS Gold O&M Assessment

ITSS Cloud Computing Service Capability Evaluation by MIIT

Network Security Assessment by CAC

CC EAL3+

HUAWEI

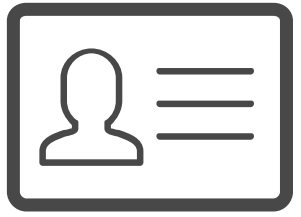
Contents

HUAWEI

Systematic Security Design

Network security

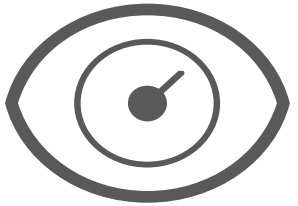
Compliance standards



Access control

Data security

Audit and tracking

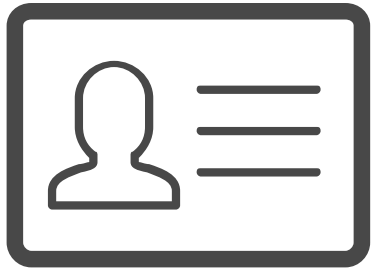


Physical infrastructure security

Event response

HUAWEI

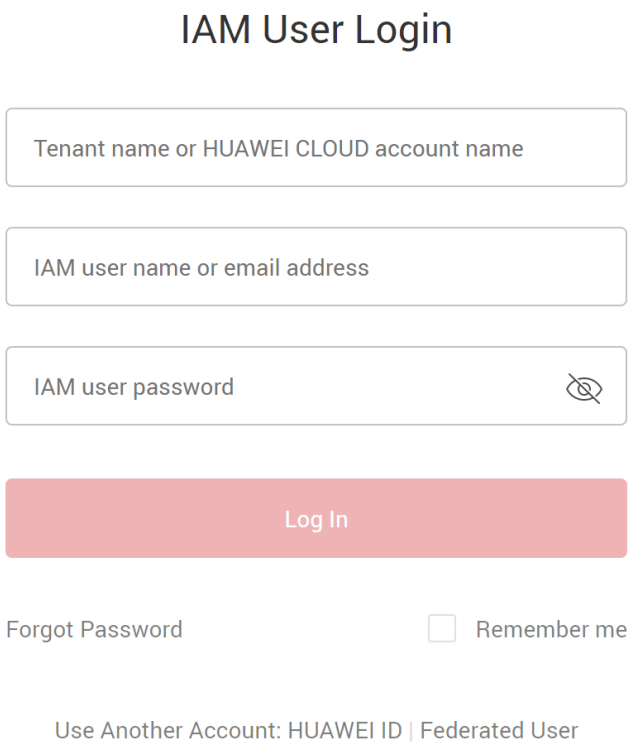
IAM Features



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



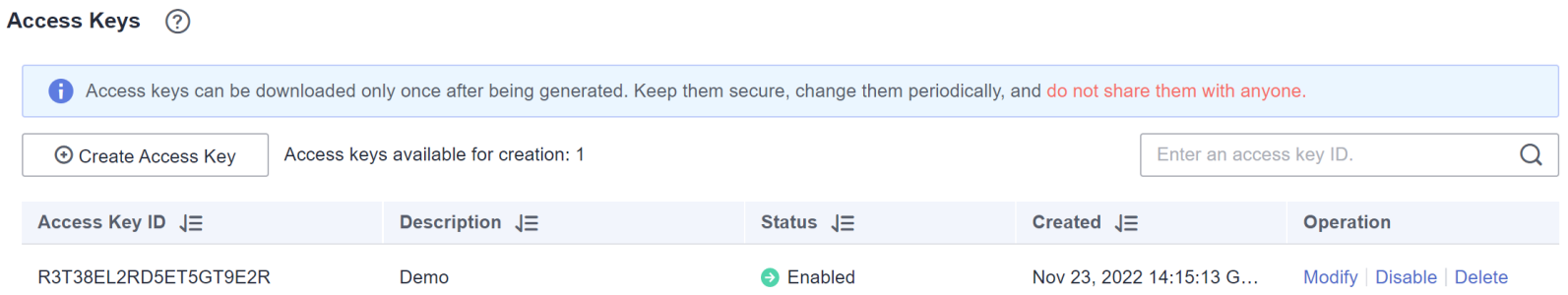
- Open the Huawei Cloud console login page.
- Use the IAM username and password to log in.
- Perform fine-grained permissions management on the IAM console.

HUAWEI

Identity Authentication Method 2

Use an access key (AK/SK) to verify your identity.

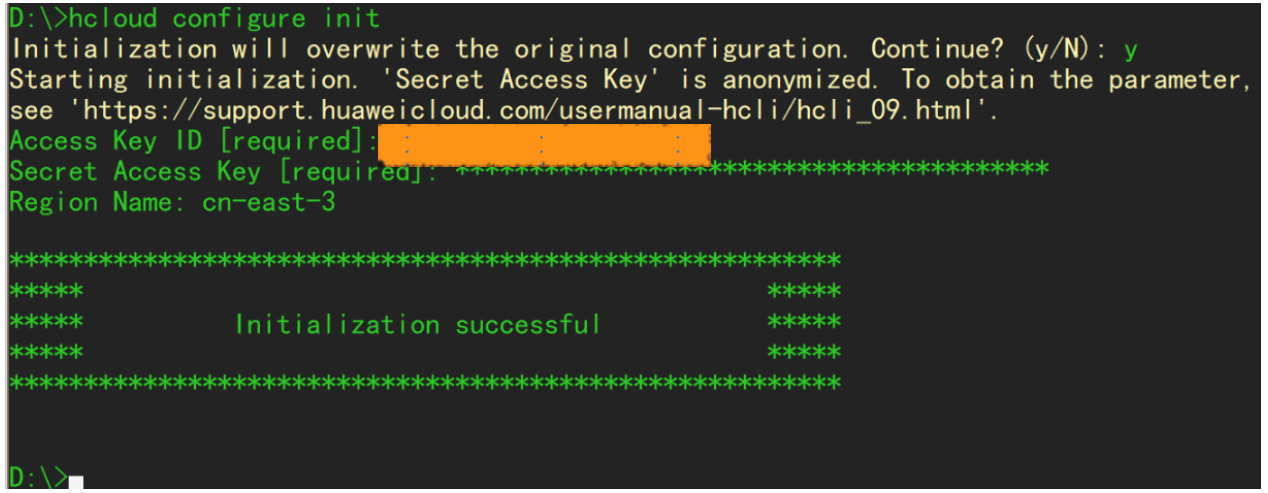
Each IAM user can create two pairs of access keys.



An AK contains 20 characters, and an SK contains 40 characters.

An AK/SK pair is used only for API access.

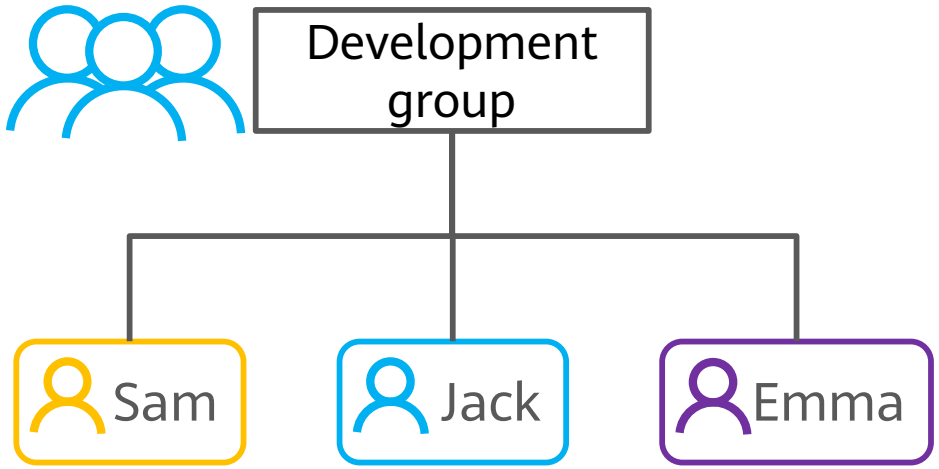
Example command in hcloud →

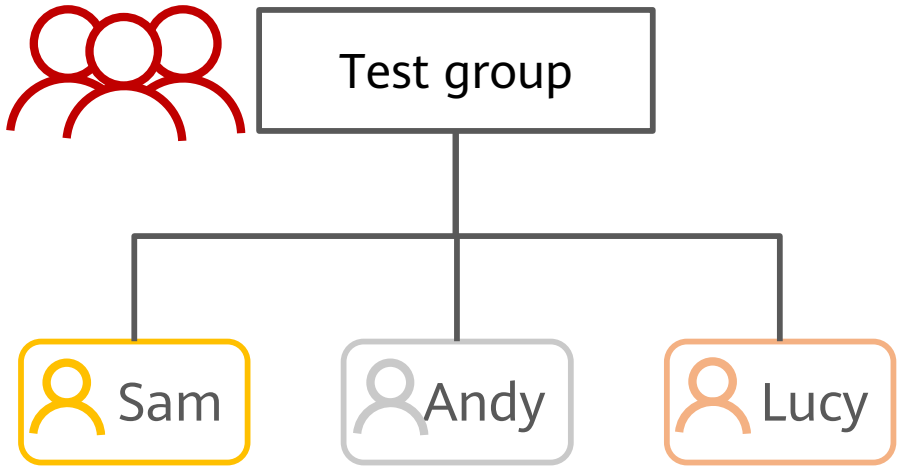


HUAWEI

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.





HUAWEI

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.

HUAWEI

IAM Policies

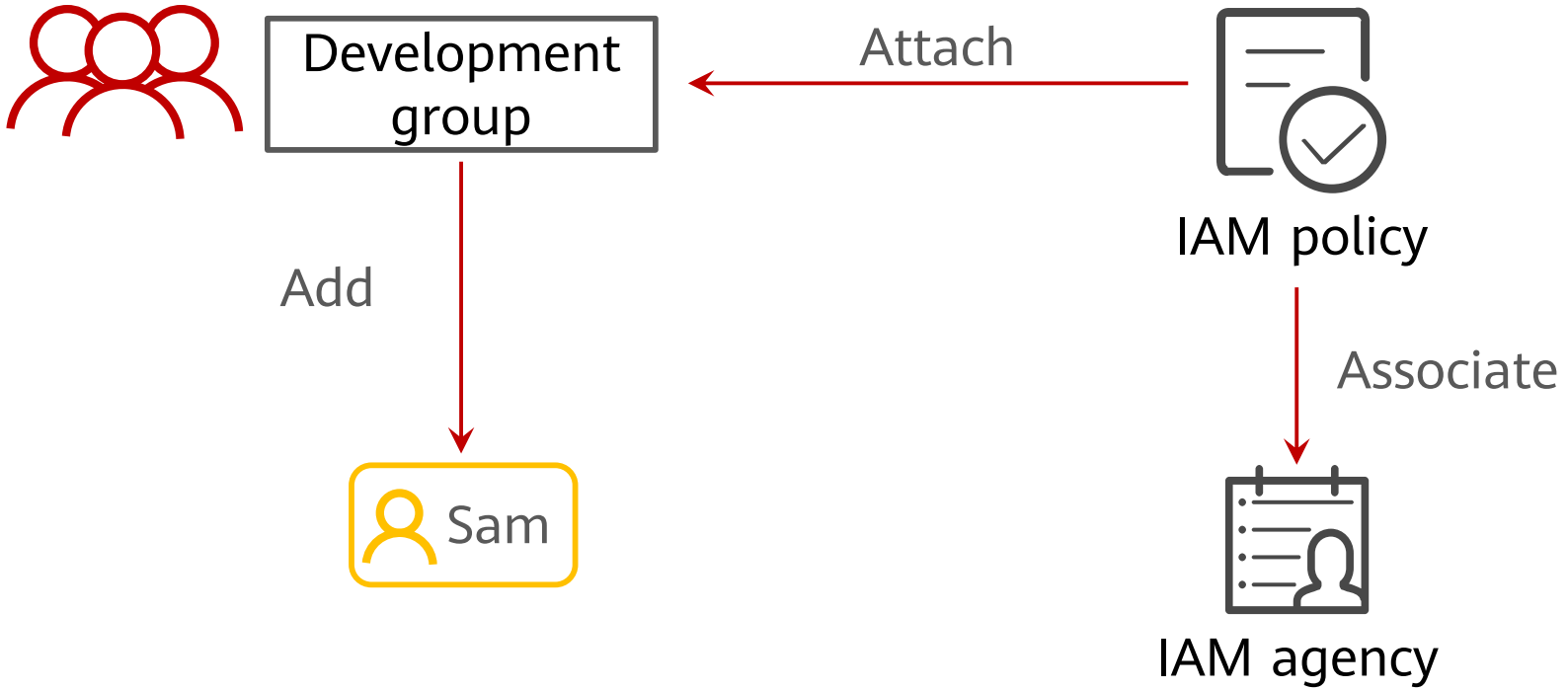
```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:ListBucket",
                "obs:bucket:Get*"
            ],
           "Resource": [
                "obs:*:*:bucket:*"
            ],
            "Condition":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

IAM policies

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

HUAWEI

IAM Policy Attachment



HUAWEI

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

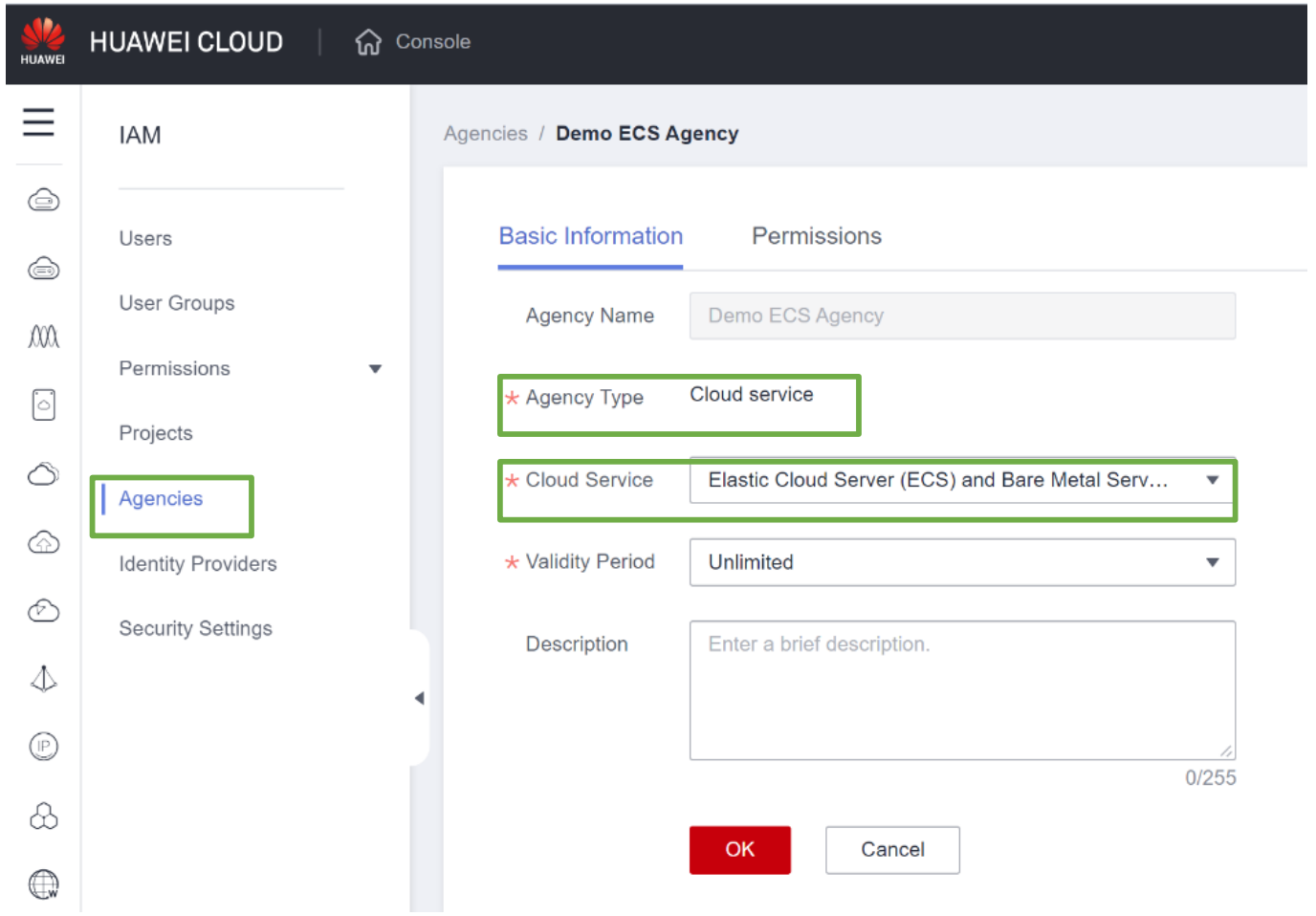
HUAWEI

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. √

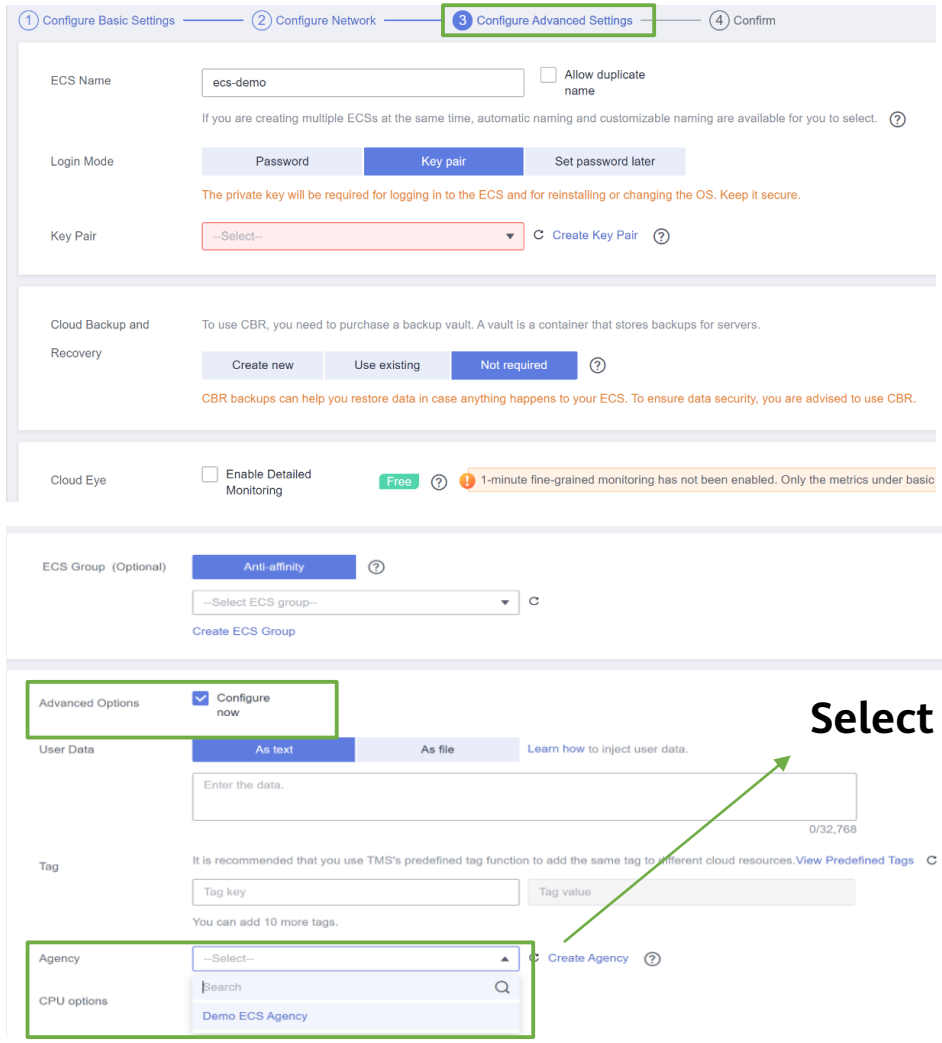
Creating an IAM Agency for ECS

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

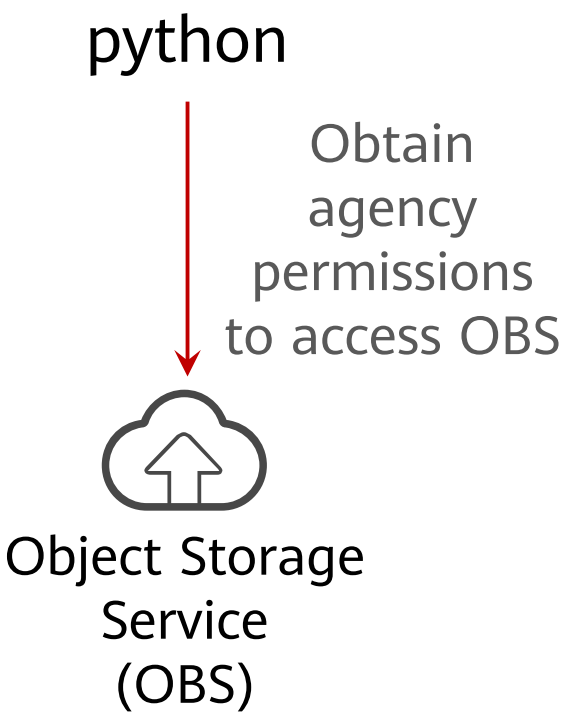


Associating the Created Agency with the ECS

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

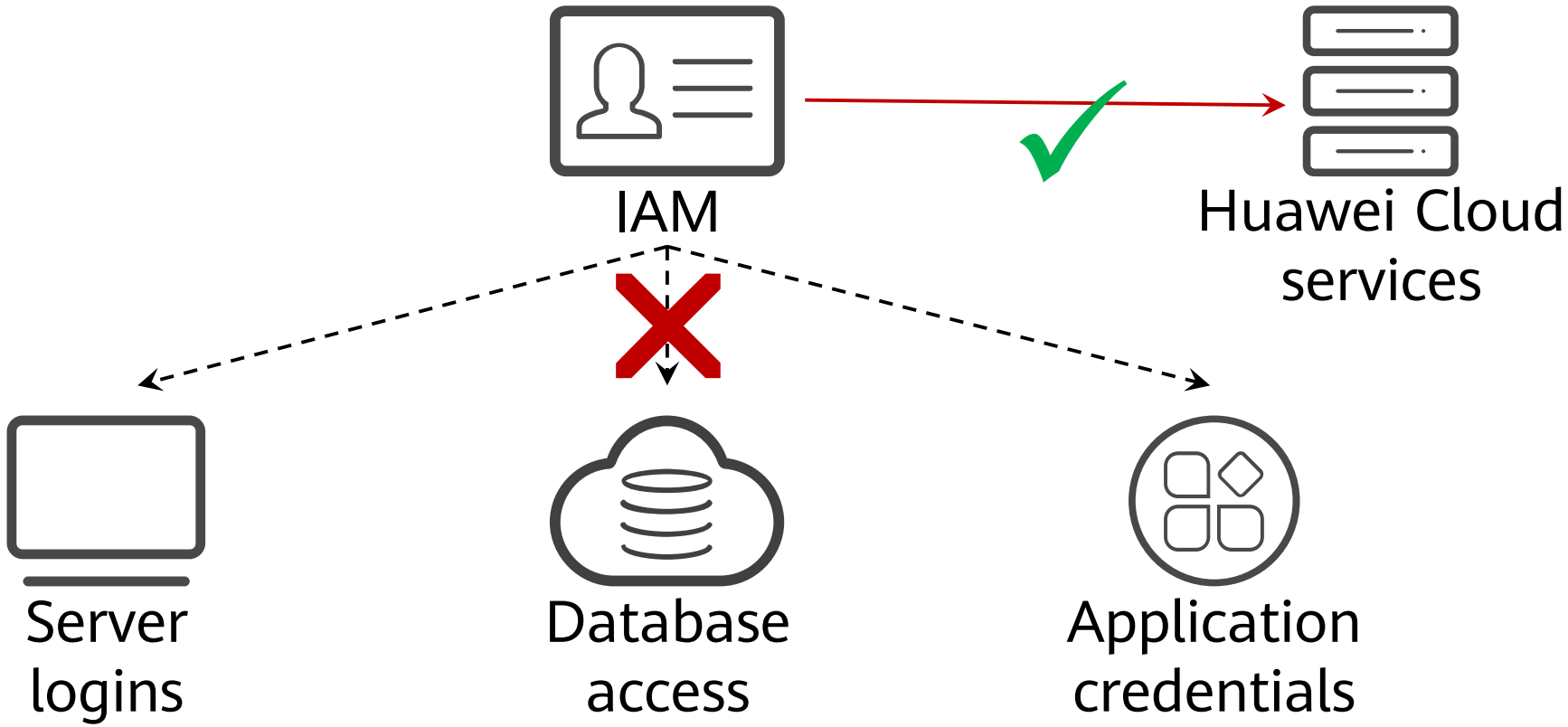


Select the ECS agency.



HUAWEI

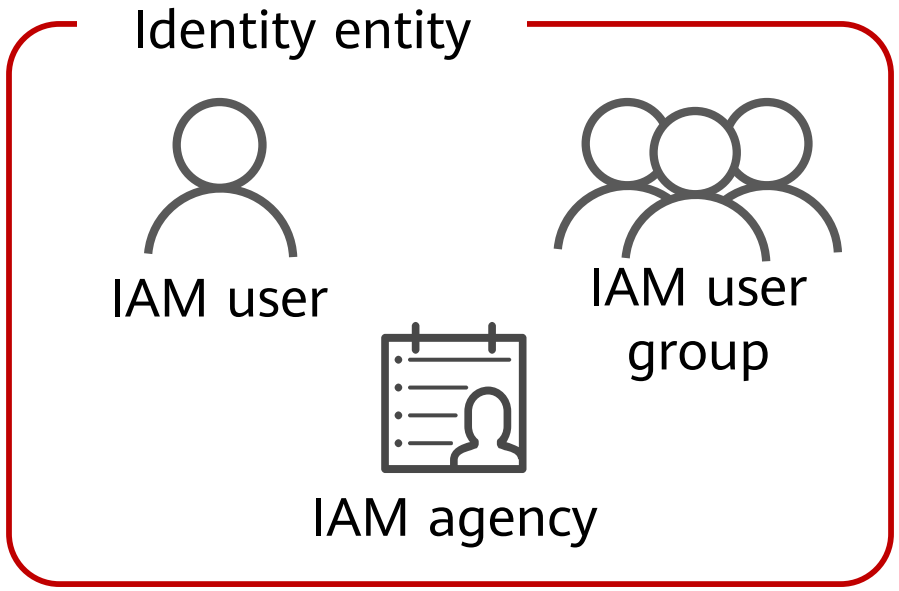
Access Control Only for Huawei Cloud Services



HUAWEI

IAM Summary

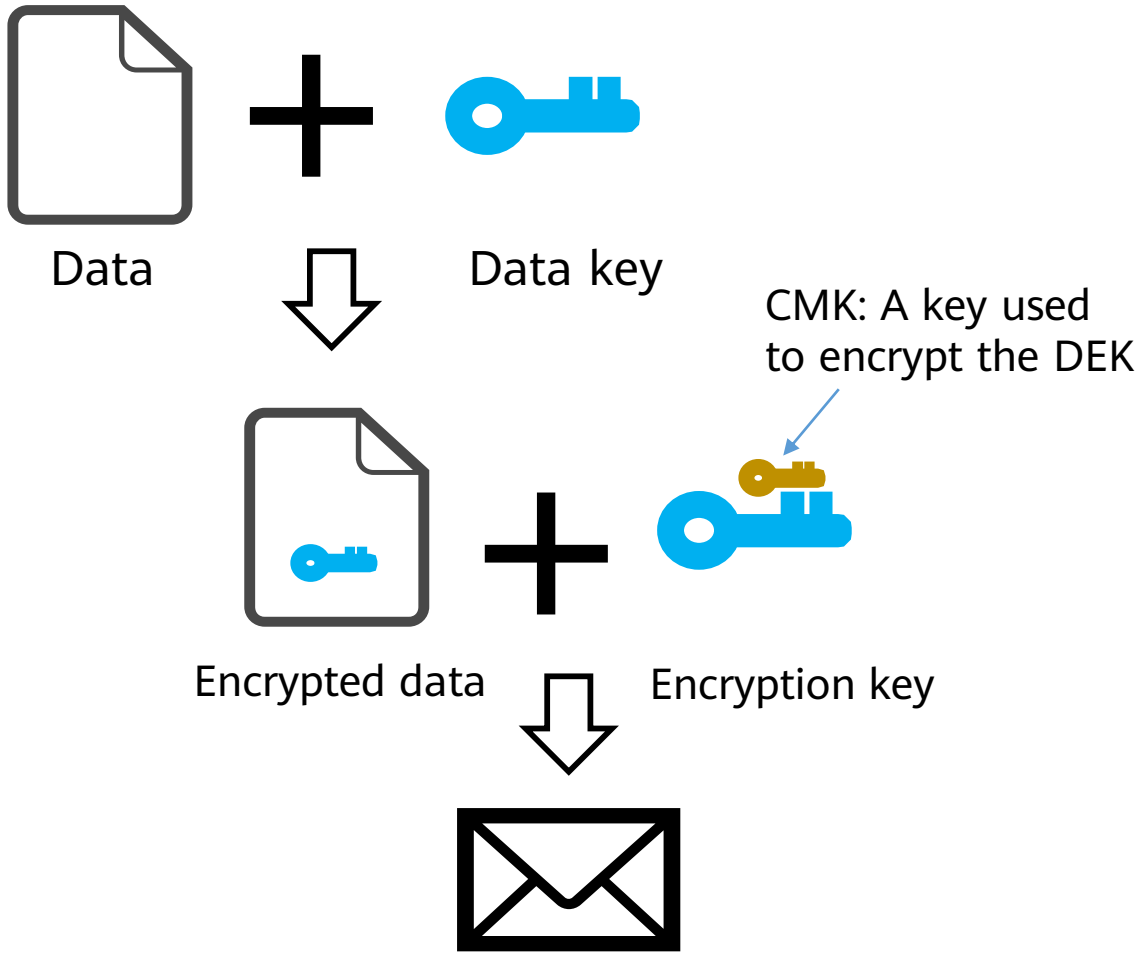
- Identity authentication
  - Console
    - Username and password
  - Programmatic access
    - AK/SK
- Access management
  - Policies defined by JSON documents



Contents

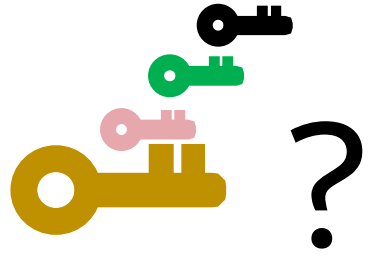
HUAWEI

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?

HUAWEI

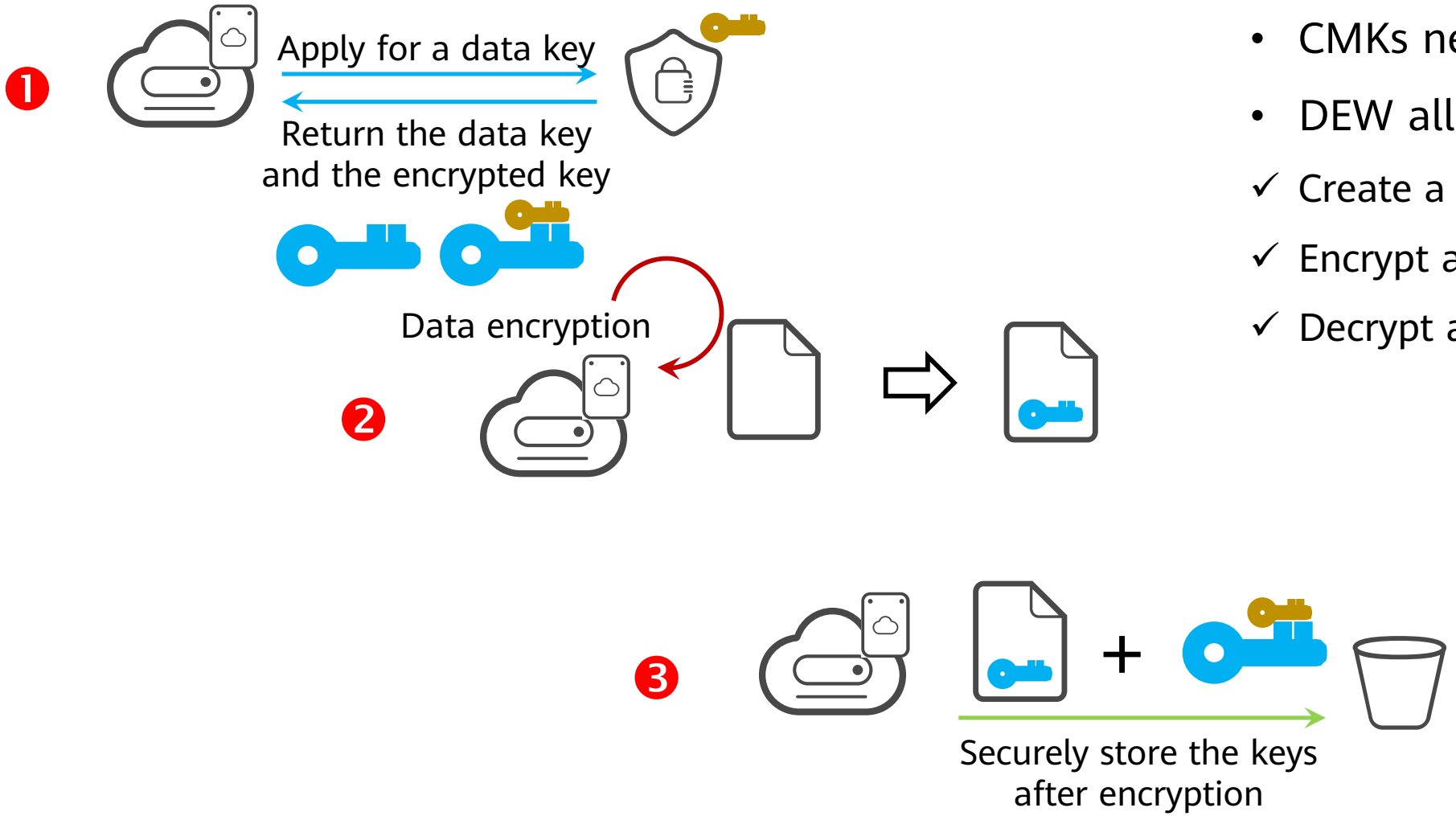
Using DEW to Manage Secrets in Applications

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

HUAWEI

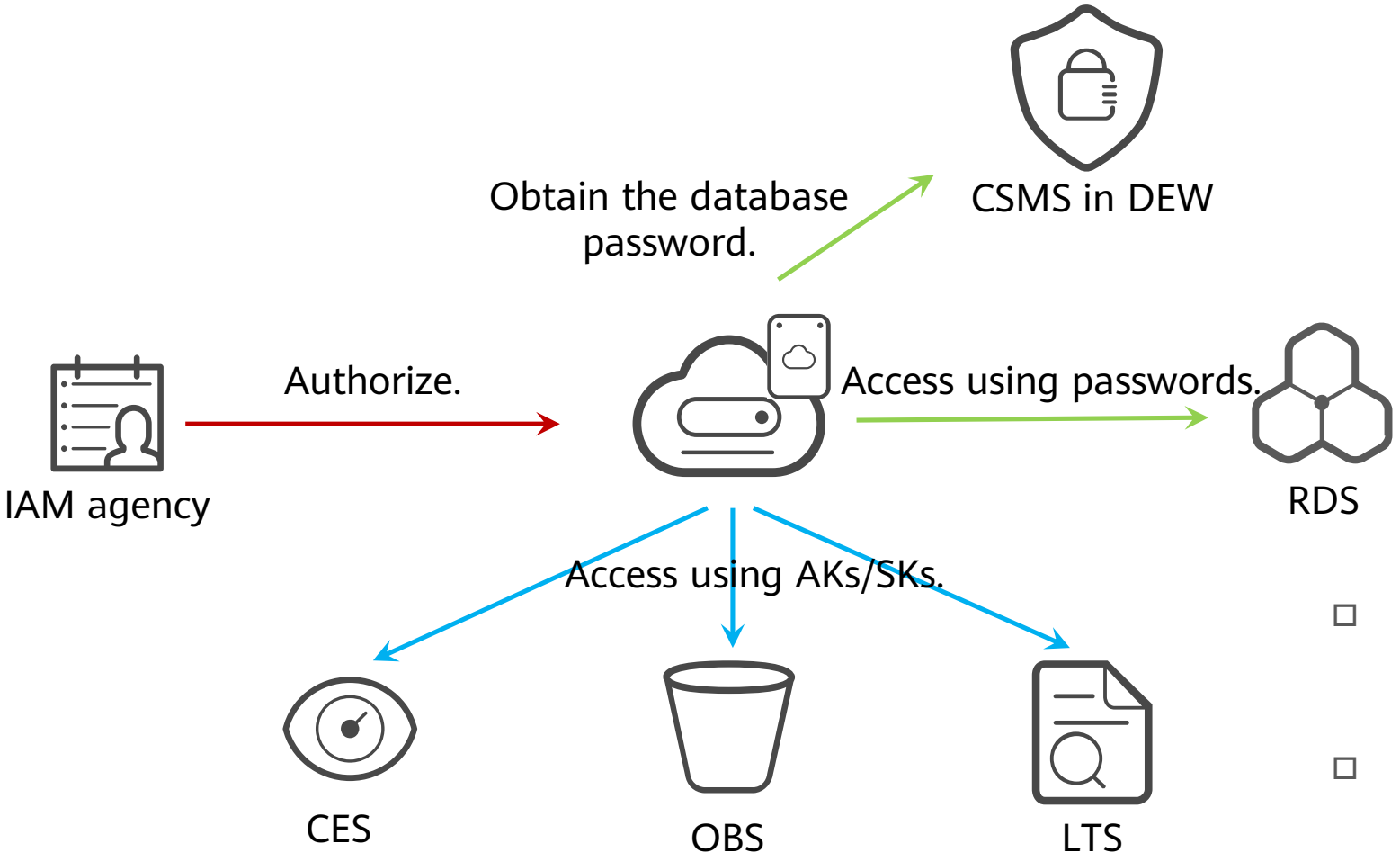
Using KMS for Data Encryption and Decryption



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

HUAWEI

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.

HUAWEI

Contents

HUAWEI

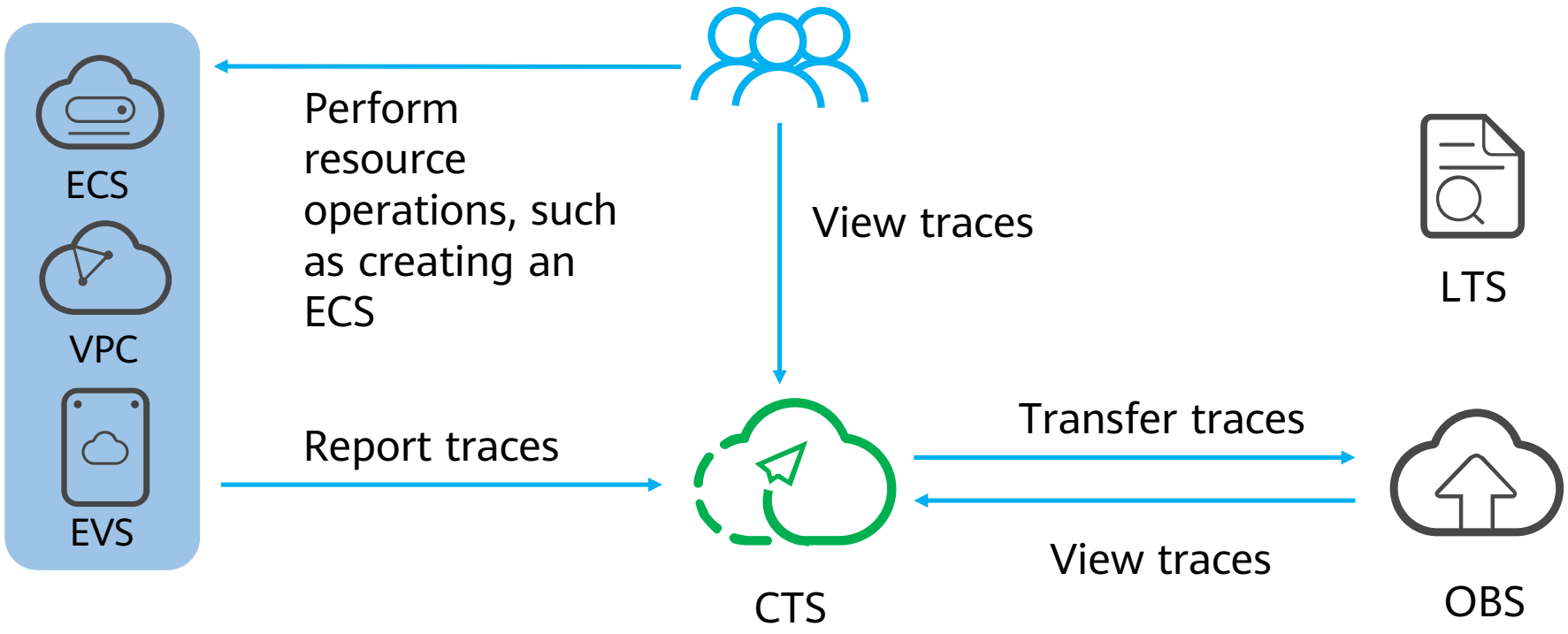
Enabling CTS

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.

HUAWEI CLOUD
EVERYTHING AS A SERVICE

www.huaweicloud.com