# General Overview of SAP Cloud Platform Infrastructure

Frank Zhao, SAP
Month 04, 2019

INTERNAL

中数通信息有限公司
China DataCom Corporation Limited

THE BEST RUN SAP®

# Agenda

Alibaba Cloud  Overview

- Account Types / Portal Websites
- Corporate Account
- Billing Methods
- Resource Access Management (RAM)
- RAM Scenarios
- Technical User
- Enable Access From Alibaba Cloud  ECS To Our Buckets
- Resource Management Interfaces
- Log in to an Instance
- Regions and Zones
- Networking
- Network layout in Cloud Platform
- Service Availability
- Quota Management, Limits, and SLA

# Agenda

## HAProxy Essential

- HAProxy basics
- HAProxy in SAP Cloud Platform
- Directing Traffic
- SSL and TLS
- Changing the Message

# Alibaba Cloud  Overview

# Account Types / Portal Websites

Alibaba Cloud  has two portals – the **Chinese (domestic)** portal and the **Global (international)** portal, which provide services for enterprises and individuals who are registered in China and abroad.

- The international portal consists of a bilingual console (English and Chinese) and a multilingual website.
- On both portals, users can browse and read about Alibaba Cloud products and services, as well as register or log on to the portal to purchase and manage their cloud services.
- However, because laws and security regulations vary from region to region and from country to country, the Chinese (domestic) portal differs from the Global (international) portal to some extent in terms of products, solutions, support services, and marketplace product offerings.
- Due to exchange rates and local tax rates, prices on the Chinese portal and Global portal may vary as well.
- Alibaba Cloud domestic account type is used for SAP CP deployments both in Frankfurt and China regions due to Chinese regulation compliance requirements and provides access to a wider set of services in comparison to an international account.

# Corporate Account

Accounts are the main organizational components in Alibaba Cloud.

Accounts provide an abstract grouping that can be used to associate resources with a particular department or a team.

All Cloud Platform resources belong to an account. Accounts provide an *isolation boundary*.

The SAP CP @ Alibaba Cloud port creates an entire CP landscape **inside a single Alibaba Cloud account**.

The resources are created within a geographical region defined in the landscape configuration.

Scoping an entire landscape to a single Alibaba Cloud project makes it easier to identify the specific resources allocated to that landscape in the Alibaba Cloud portal and command-line utilities.

# Billing Methods

- Alibaba Cloud employs different billing methods and prices for different services, two main methods of billing are:
  - Subscription – more economical for long term usage
    - o The yearly/monthly purchase is payment and settlement model used in the pre-paid model.
    - o The yearly/monthly subscription based instances support anytime configuration upgrade.
  - Pay-as-you-go – better for agile or scaling environments
    - o The Alibaba Cloud PAYG model is similar to AWS EC2 PAYG model, which is based on post-paid payment.
- Important notes:
  - SAP CP also uses a PAYG model for resources, which allows resource creation and release on demand.
  - **Subscription resources cannot be released or deleted until the subscription expires.**

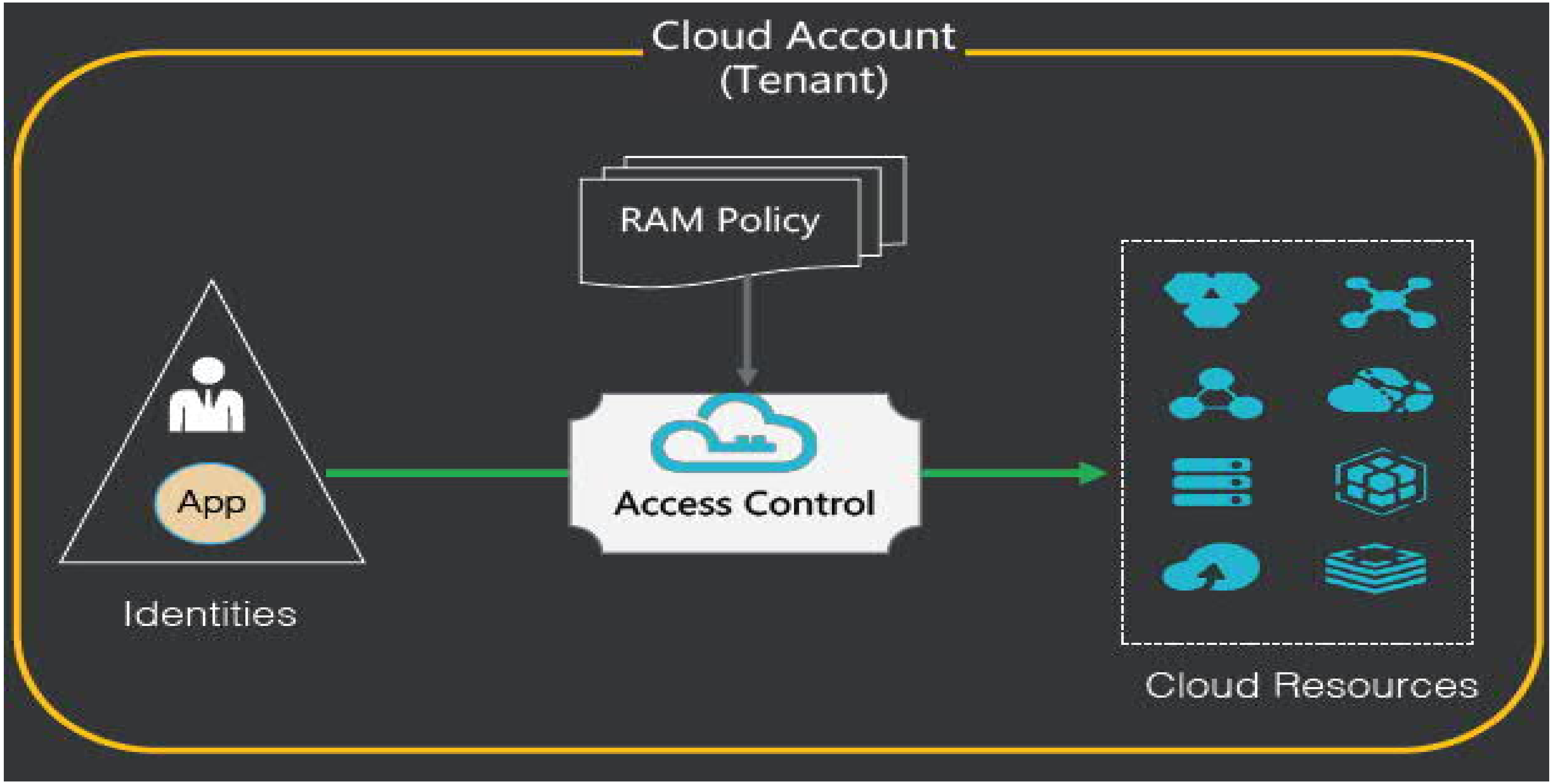
# Access Management

Alibaba Cloud resource access management (RAM) is a management service designed for the centralized management of cloud identities and access permissions.

You can use RAM to grant access and management permissions to Alibaba Cloud resources.

| Functionality | Alibaba Cloud RAM |
|---|---|
| User/Policy/Group/Role management | Supported |
| Operation audit | Supported |
| Security | Token, access key |

# RAM Overview



# Identity

An identity refers to any person, system, or application that uses resources in the RAM console or through open APIs. To manage identities in different application scenarios, RAM supports two types of identities, RAM users and RAM roles.

- A RAM user is an entity identity with a fixed ID and an identity authentication key. Generally, a RAM user corresponds to a person or an application.

- A RAM role is a virtual identity with a fixed ID but without an identity authentication key.

A RAM role must be associated with an entity identity before it can be used. A RAM role can be associated with multiple entity identities, such as:

- RAM users under the current account

- RAM users under another account

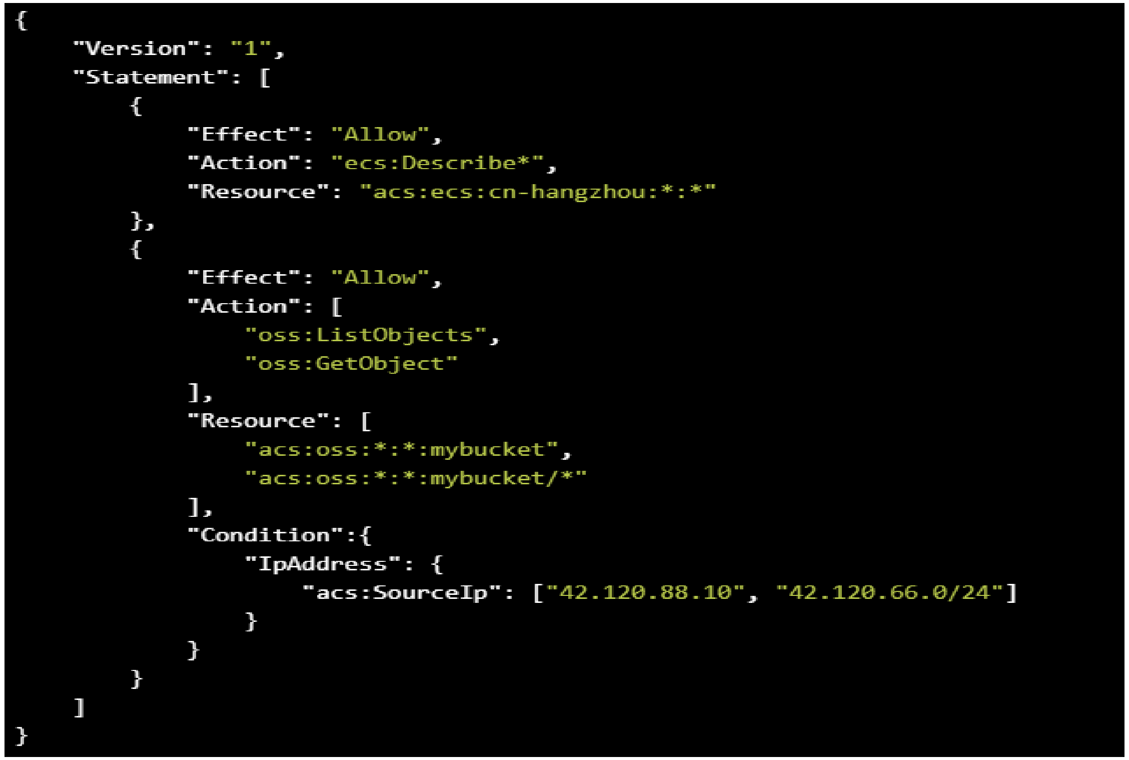
- Alibaba Cloud services (such as EMR or MTS)

- External real identities (such as a local enterprise account)

# Policy

RAM allows you to create and manage multiple policies under your account. In essence, each policy is a collection of permissions. Administrators can attach one or more policies to a RAM identity (a RAM user or RAM role).

The RAM policy language expresses fine-grained authorization semantics. A policy can grant permissions to a specific API action or resource ID and specify multiple restrictions (such as source IP address, access time, and MFA).



```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ecs:Describe*",
            "Resource": "acs:ecs:cn-hangzhou:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:mybucket",
                "acs:oss:*:*:mybucket/*"
            ],
            "Condition":{
                "IpAddress": {
                    "acs:SourceIp": ["42.120.88.10", "42.120.66.0/24"]
                }
            }
        }
    ]
}
```

# Relationship between accounts and RAM users

- From the ownership perspective, an account and its RAM users are in parent-child relationship.

- An account is the basic entity for judging the ownership of Alibaba Cloud resources and billing for resource consumption.

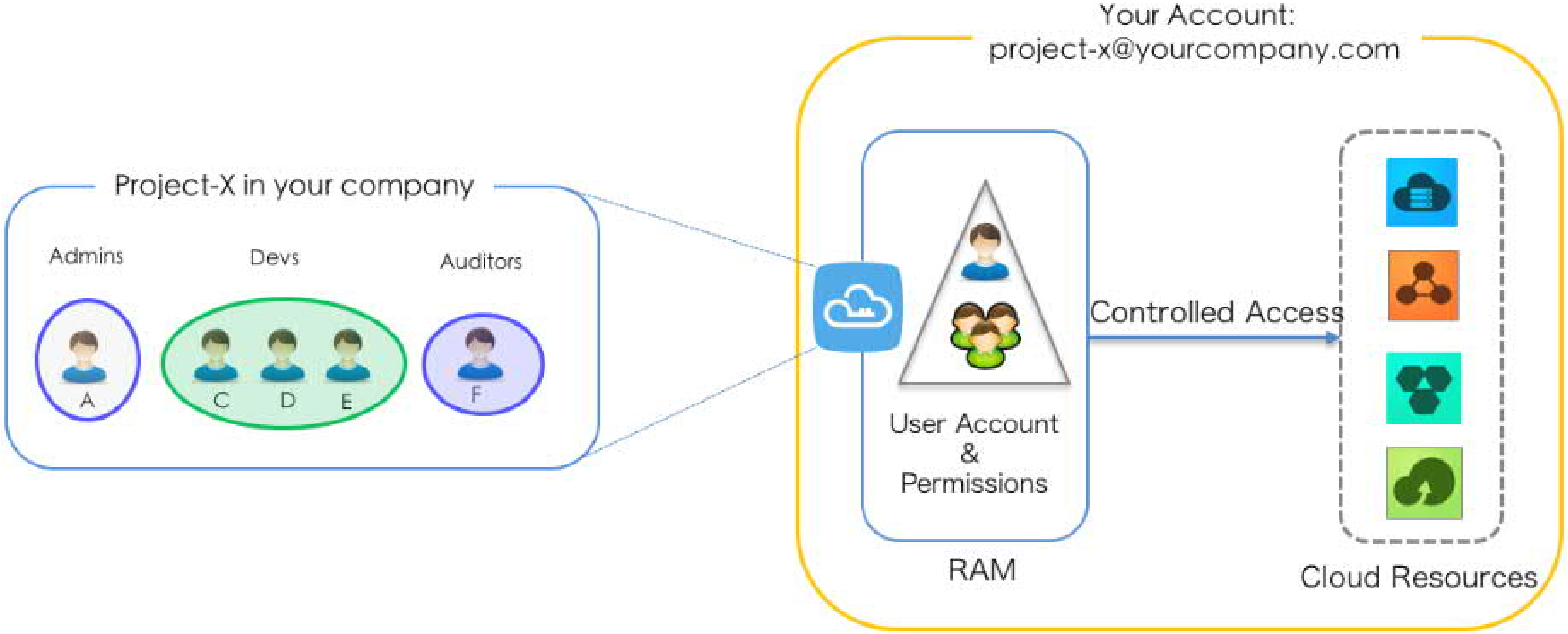
- RAM users exist only in RAM instances of a certain account. RAM users do not possess resources, and the resources they create under authorization belong to their accounts. RAM users do not possess bills, and all fees incurred by their authorized operations are debited to their accounts.

- From the permission perspective, an account and its RAM users are in root–user relationship (similar to the relationship in Linux).

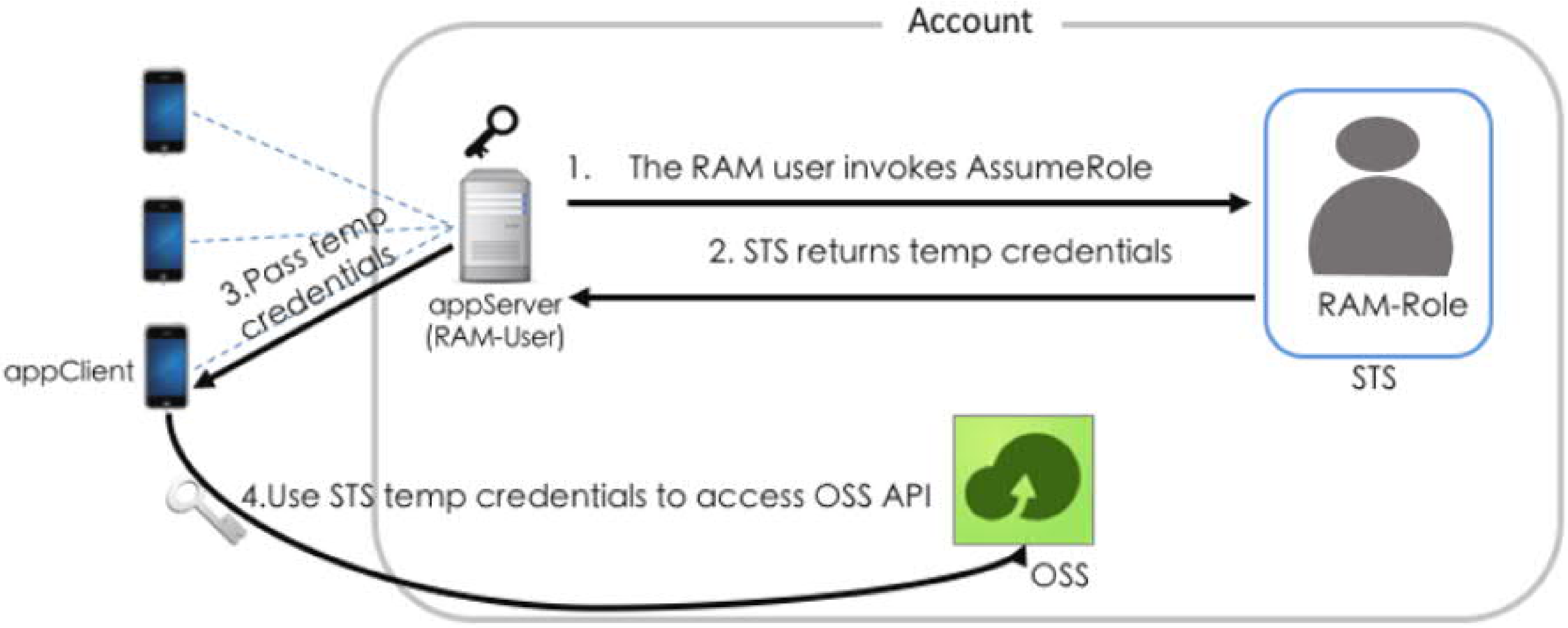
- The root user has all operation and control permissions on resources.

- RAM users only have permissions that are granted by the root user. The root user can revoke the permissions at any time.

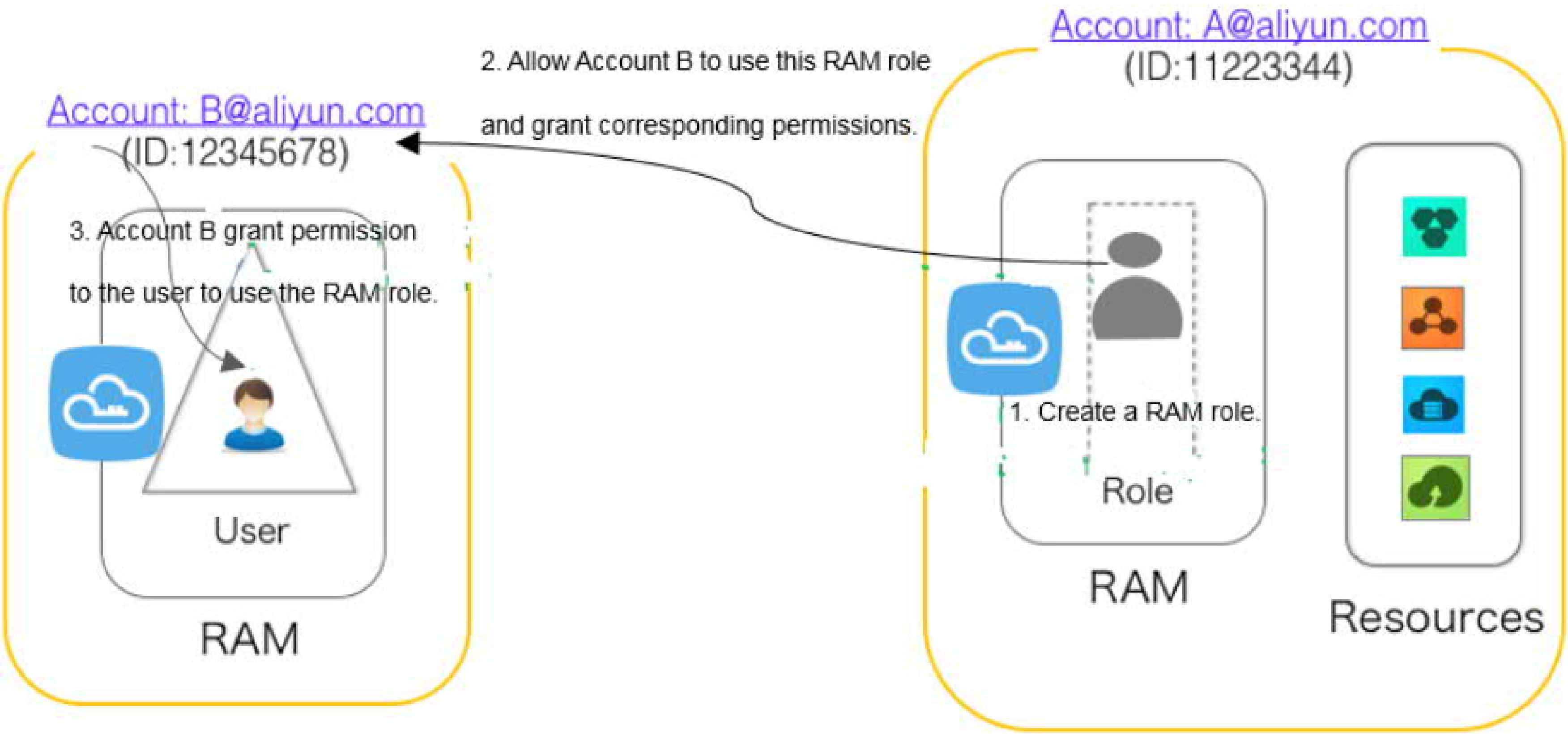
# Scenarios-User management and access control



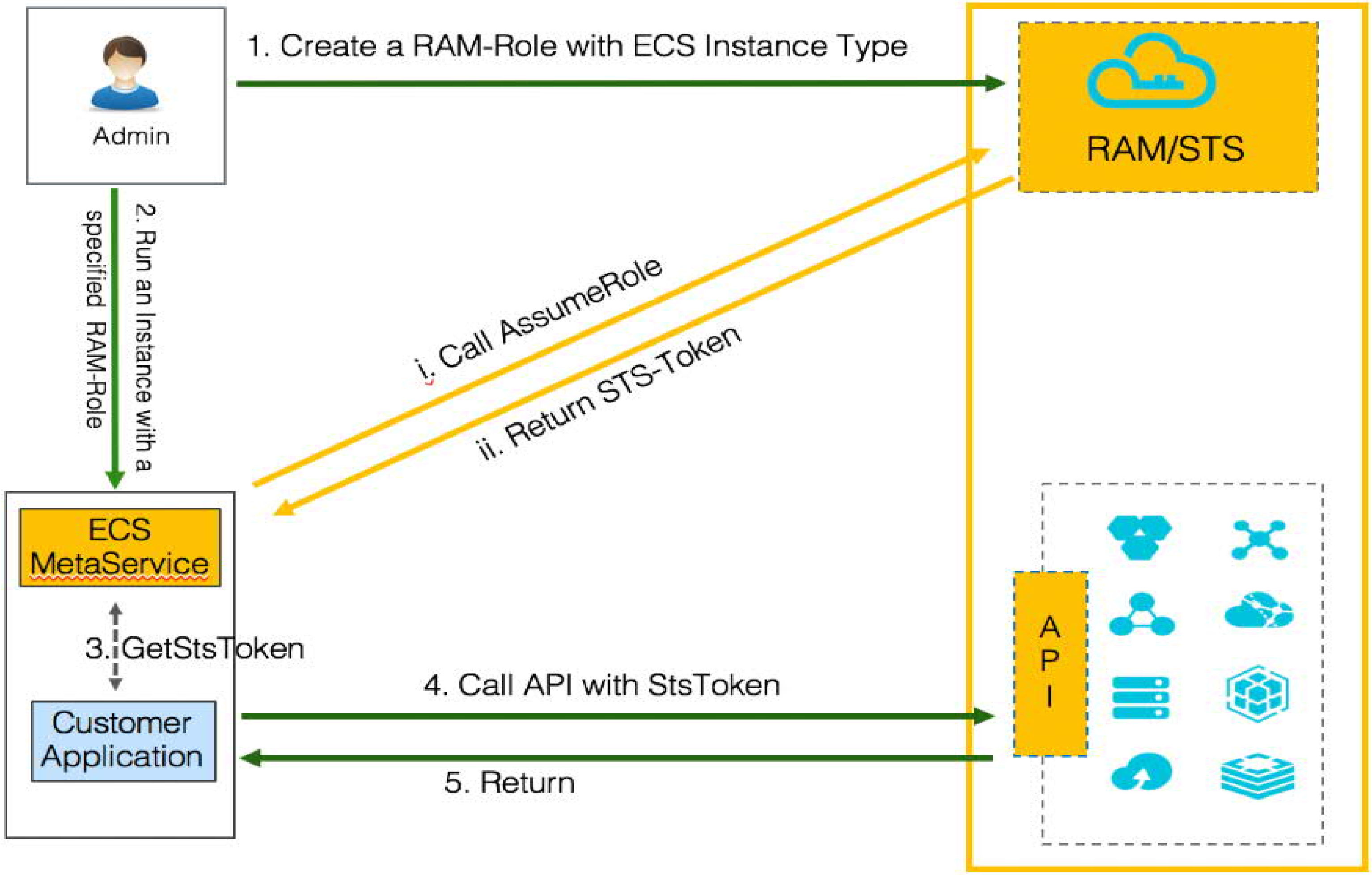
# Scenarios-Grant temporary permissions to mobile apps


Account
1. The RAM user invokes AssumeRole
2. STS returns temp credentials
3.Pass temp credentials
4.Use STS temp credentials to access OSS API
appServer (RAM-User)
appClient
RAM-Role
STS
OSS

# Scenarios-Cross-account resource authorization and access


Account: B@aliyun.com
(ID:12345678)
2. Allow Account B to use this RAM role
and grant corresponding permissions.
Account: A@aliyun.com
(ID:11223344)
3. Account B grant permission
to the user to use the RAM role.
User
RAM
1. Create a RAM role.
Role
RAM
Resources

# Scenarios-Dynamic identity and permission management of cloud applications



# Technical User

The Access/Secret key credentials can be created in RAM (user center) for programmatic access to the resources using Terraform or Alibaba Cloud CLI/SDK.

The following roles only should be assigned to the SAP CP technical user used in deployment by bosh CPI and Alibaba Cloud Terraform provider:

- ❑ AliyunOSSFullAccess
- ❑ AliyunECSFullAccess
- ❑ AliyunRDSFullAccess
- ❑ AliyunSLBFullAccess
- ❑ AliyunVPCFullAccess
- ❑ AliyunEIPFullAccess
- ❑ AliyunCloudMonitorFullAccess
- ❑ AliyunNATGatewayFullAccess

# Enable Access From Alibaba Cloud  ECS To Our Buckets For Creating Stemcells

- Log on to the ECS console.
- In the left-side navigation pane, choose Snapshots and Images > Images.
- Click Import Image.
- In the Import Image dialog box, click Confirm Address as follows.
- In the Cloud Resource Access Authorization window, select AliyunECSImageImportDefaultRole and AliyunECSExportDefaultRole, then click Confirm Authorization Policy to allow the ECS service to access your OSS resources.

Follow this link Under procedure: steps 2-6
https://www.alibabacloud.com/help/doc-detail/25464.htm

# Resource Management Interfaces

- Alibaba Cloud provides a web-based console for resource management, but there are additional resource management interfaces available such as REST API and command line interface (CLI).

- The developer is able to perform operational tasks like VM creation, disk attachment, etc. by using these tools.

Alibaba Cloud resources can be managed in one of the following ways:

- The Alibaba Cloud portal — https://home.console.aliyun.com/
- Aliyun CLI tools for manual devops — https://github.com/aliyun/aliyun-cli
- Terraform with Alibaba Cloud provider — https://www.terraform.io/docs/providers/Alibaba Cloud /index.html
- BOSH with Alibaba Cloud CPI — https://github.com/cloudfoundry-incubator/bosh-Alibaba Cloud -cpi-release

# Log in to an Instance

- In Alibaba Cloud, the connection to the VM instance is possible through SSH protocol and also via Management Terminal.
- To utilize the SSH connection, the SSH key should be created and associated to a VM in advance.
- It is possible to connect to the VM using login/password, but this option should be considered from the security perspective.
- The management terminal provides VNC connection to the machine and direct login to the VM terminal console. This option can be useful for the collection of logs from the operation system and identification of boot errors.

In addition to the regular ssh connection using private-key credentials, Alibaba Cloud also provides a VNC connection from the portal to the ECS instances. While this functionality might be useful in some investigation cases, with instances deployed by BOSH, you are not allowed to log in using this method, even if the password reset operation was applied.

Only instances created manually with a predefined user password allow login using VNC connection.

# Regions and Zones

- Alibaba Cloud uses the same concept and terminologies: regions and zones
  - Regions are located in different locations around the world.
  - Zones are physical areas within the same region but with independent power grids and networks.

| Element | AWS Term | Alibaba Cloud Term |
|---|---|---|
| Cluster of data centers and services | Region | Region |
| Abstracted data center | Availability Zone | Zone |
| Edge node | Edge Network Location | Edge Node |

# Networking

| Alibaba Cloud | Description |
|---|---|
| Virtual Private Cloud | Construct a logically isolated networking environment where you can customize your CIDR ranges, subnets, routes, and network gateways. |
| Express Connect | Establish a dedicated network connection from an on-premise environment to cloud services and also between cross-regional VPCs and between cross-account VPCs. |
| Server Load Balancer | Distribute traffic among several cloud servers. |
| Cloud DNS | DNS management services. |

# Network layout

- Main network layout
- Layout of the CF core networks
- Platform networks
- Service networks
- Infrastructure Networks

Network Layout

# Service Availability

- The availability of regions and zones does not apply to all products of Alibaba Cloud.

- The zones of some services are transparent to users, such as for Object Storage Service (OSS or blob storage) and Elastic Compute services (ECS) images.

- Some other services run on multiple regions by default, such as DNS and CDN.

# Cloud Service Types

| Category | Alibaba Cloud |
|---|---|
| Computing | • ECS (elastic compute service)<br>• Container Service |
| Storage | • ECS Disk<br>• OSS (object storage services)<br>• NAS (network attached storage) |
| Network | • VPC<br>• Express Connect<br>• Elastic IP<br>• SLB (server load balancer) |
| Database | • ApsaraDB for RDS |

# Additional Services

| Category | Alibaba Cloud |
|---|---|
| Security services | • Anti-DDoS Basic/Pro<br>• WAF<br>• Server Guard |
| Management services | • Cloud Monitor<br>• RAM (resource access management)<br>• KMS (key management service) |
| Domains & Websites | • Cloud DNS<br>• Cloud Web Hosting |
| Email | • Direct Mail |

# Quota Management, Limits, and SLA

- The status of the quota limits and usage can be monitored on the Privileges page
  – https://ecs-eu-central-1.console.aliyun.com/#/privileges/detail

- In most cases, the quota is set per region, while some resources like security group limits can be set globally on the account level.

- The full set of the limits is available on https://www.alibabacloud.com/help/doc-detail/54462.htm.

- A few important limits:
  - ❑ Security groups per VM – 5 by default, 16 upper limit.
    For correct SAP CP deployment the maximal limit should be applied.

  - ❑ Security groups for VPC instances: 2,000 private IP addresses (shared by primary and secondary network cards)

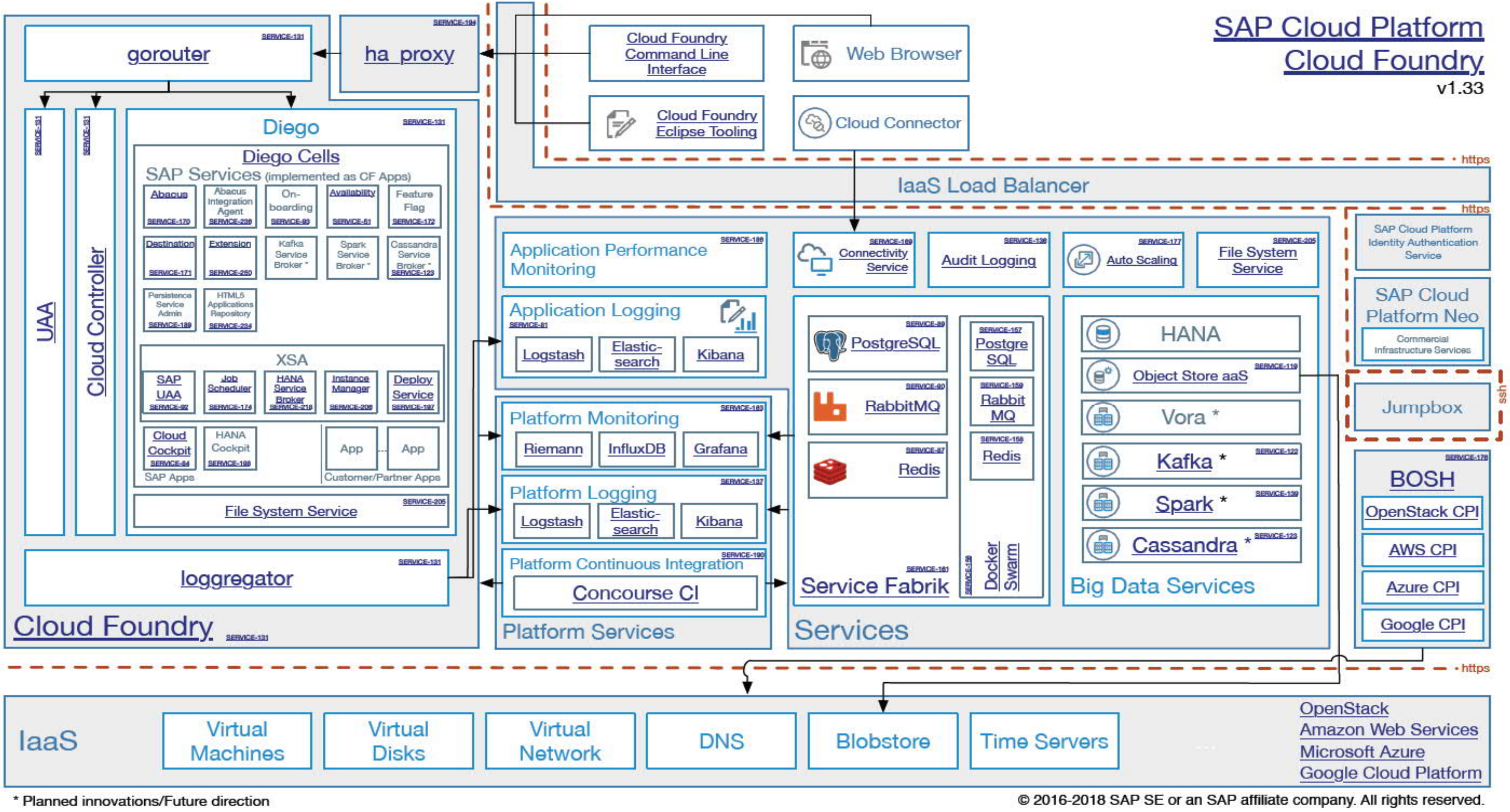
- The full set of SLA is available at https://www.alibabacloud.com/help/faq-list/42389.htm

# HAProxy

# HAProxy basics

- Load balancing basics
- TCP vs HTTP mode
- Capturing the client's IP address
- Using ACLs

# HAProxy in CP



* Planned innovations/Future direction

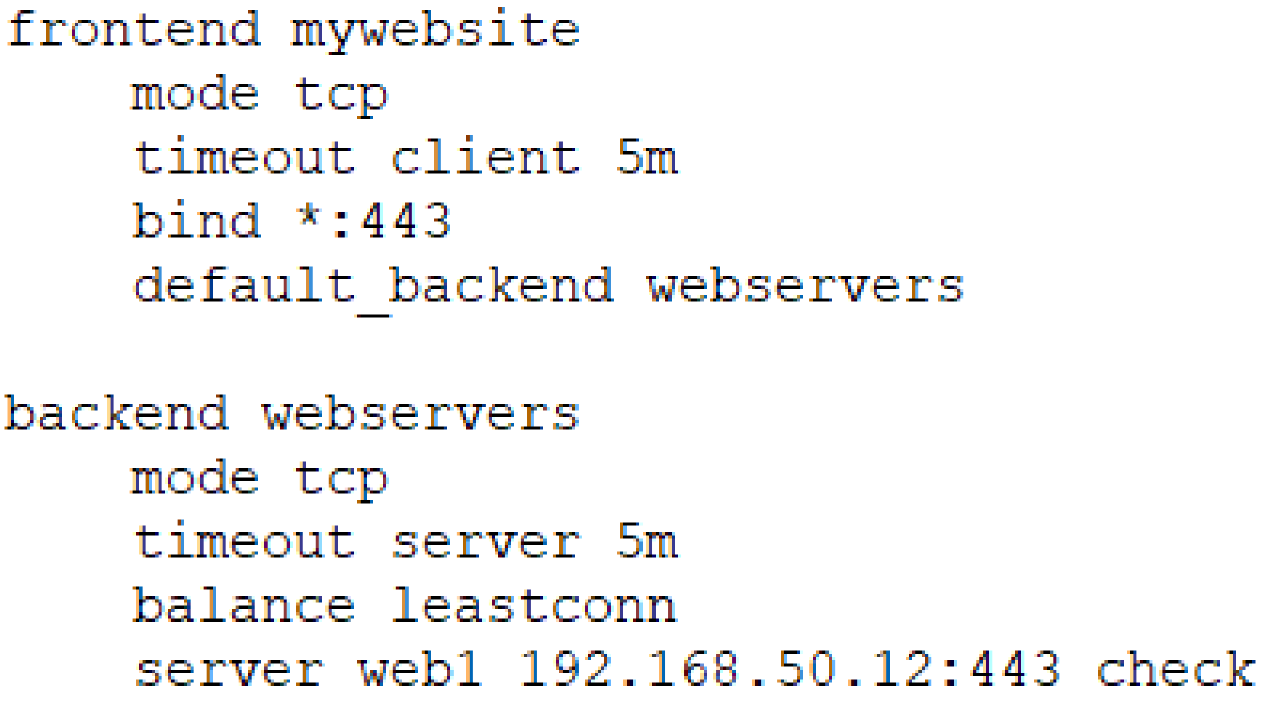
# Directing Traffic

- Content switching on the URL path
- Content switching on a URL
- Parameter
- Content switching on an HTTP
- Header
- Redirecting to another URL
- Redirecting based on geolocation

# SSL and TLS

- TLS Passthrough
- TLS termination
- TLS re-encryption
- Redirecting HTTP traffic to HTTPS

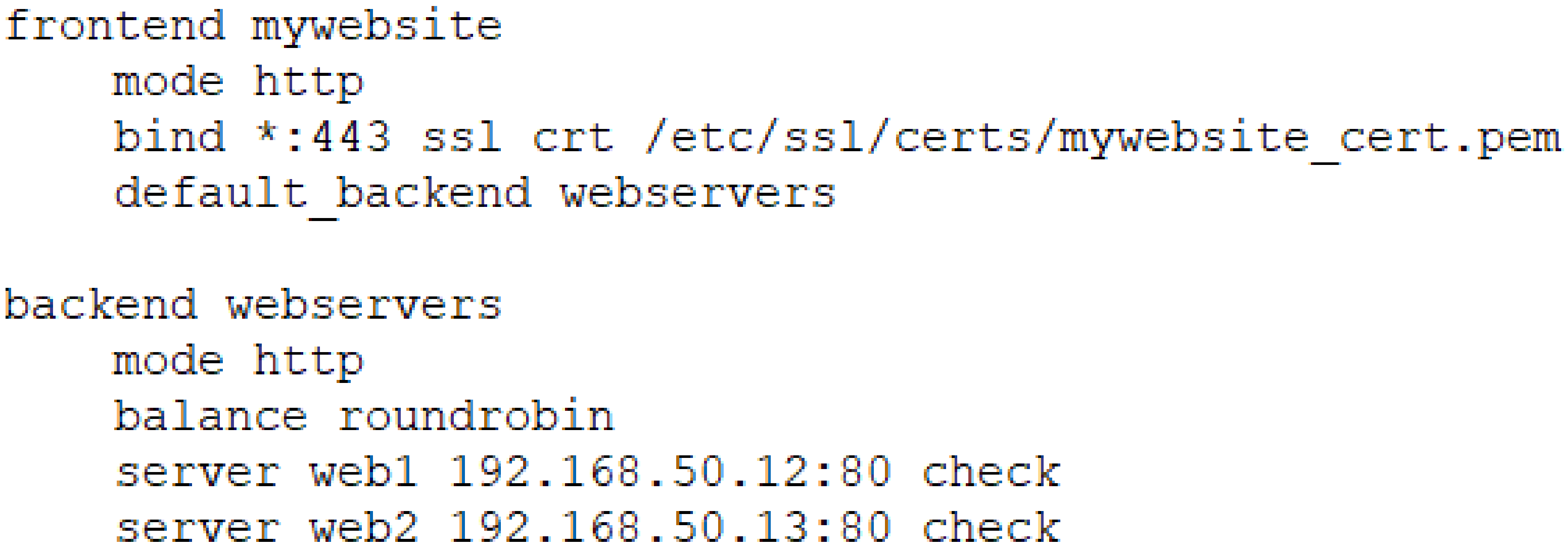
# SSL and TLS-TLS Passthrough



```
frontend mywebsite
    mode tcp
    timeout client 5m
    bind *:443
    default_backend webservers

backend webservers
    mode tcp
    timeout server 5m
    balance leastconn
    server web1 192.168.50.12:443 check
```

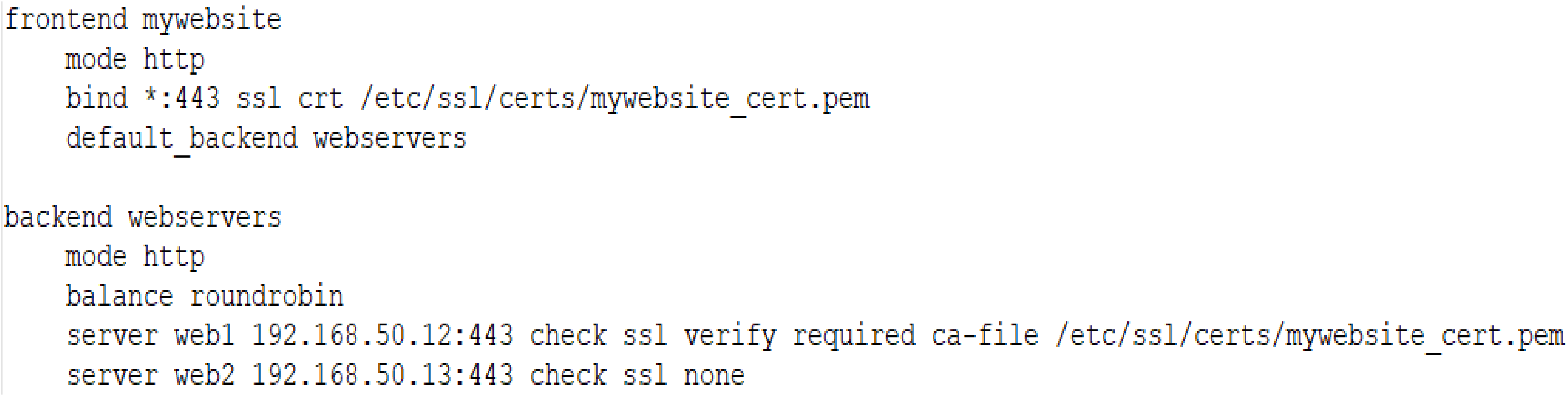
# SSL and TLS-TLS termination



```
frontend mywebsite
    mode http
    bind *:443 ssl crt /etc/ssl/certs/mywebsite_cert.pem
    default_backend webservers

backend webservers
    mode http
    balance roundrobin
    server web1 192.168.50.12:80 check
    server web2 192.168.50.13:80 check
```

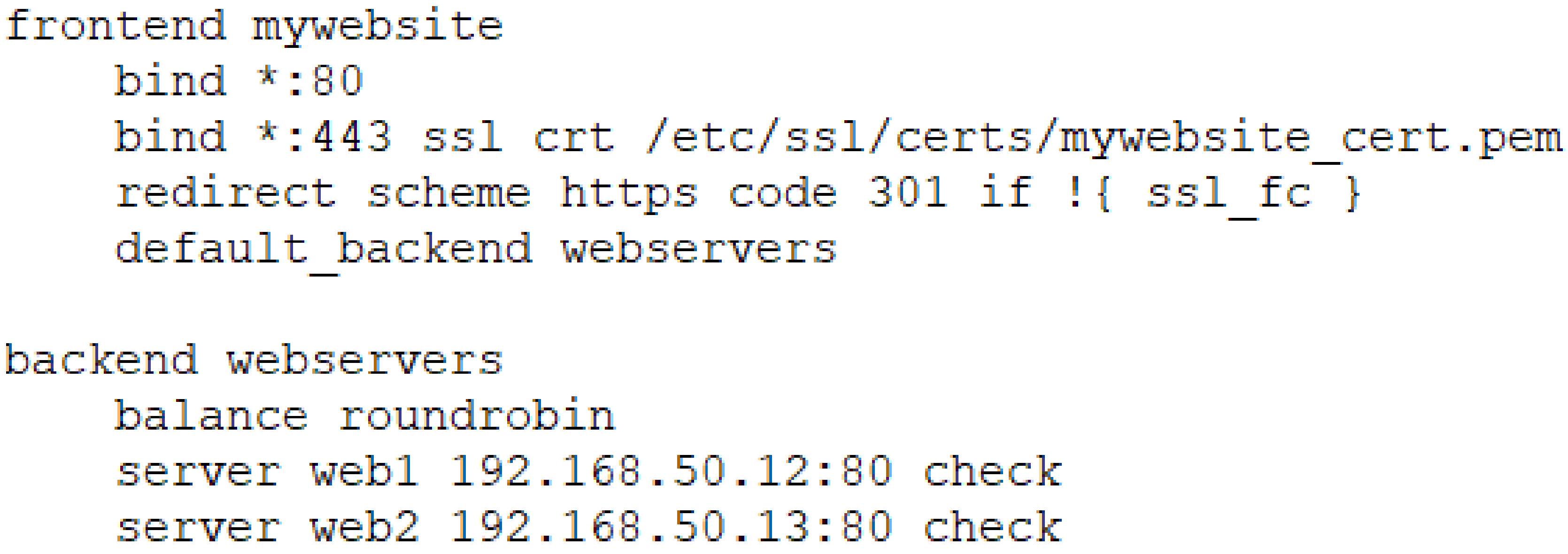
# SSL and TLS-TLS re-encryption



```
frontend mywebsite
    mode http
    bind *:443 ssl crt /etc/ssl/certs/mywebsite_cert.pem
    default_backend webservers

backend webservers
    mode http
    balance roundrobin
    server web1 192.168.50.12:443 check ssl verify required ca-file /etc/ssl/certs/mywebsite_cert.pem
    server web2 192.168.50.13:443 check ssl none
```

# SSL and TLS-Redirecting HTTP traffic to HTTPS



```
frontend mywebsite
    bind *:80
    bind *:443 ssl crt /etc/ssl/certs/mywebsite_cert.pem
    redirect scheme https code 301 if !{ ssl_fc }
    default_backend webservers

backend webservers
    balance roundrobin
    server web1 192.168.50.12:80 check
    server web2 192.168.50.13:80 check
```

# Changing the Message

- URL rewriting
- Adding request headers
- Adding response headers
- Removing response headers

# Reference Material

# Links

- ECS instances metadata: https://www.alibabacloud.com/blog/594351
- Security group limits: https://www.alibabacloud.com/help/doc-detail/101348.htm?spm=a2c63.p38356.b99.231.5eca7945JLC5Kj
- RAM user management: https://www.alibabacloud.com/help/doc-detail/93720.htm?spm=a2c63.p38356.b99.23.4f29744acYfxeM

# Thank you.

Contact information:

**Frank.zhao03@sap.com**