HUAWEI

Building a Fully Connected, Intelligent World

HUAWEI CLOUD Everything as a Service

ABSA HCS Landing Zone Design

2026, HUAWEI, South Africa

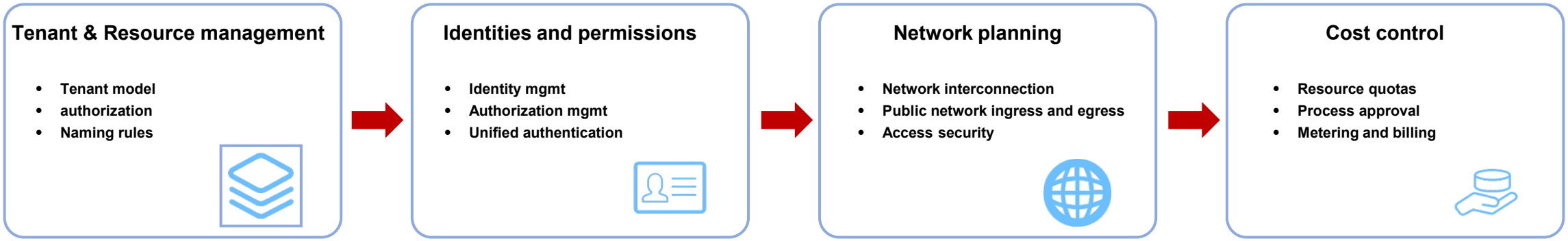
Your story matters

absa

HUAWEI CLOUD
The AI Pioneer in Industries

ABSA—HCS Landing Zone Design

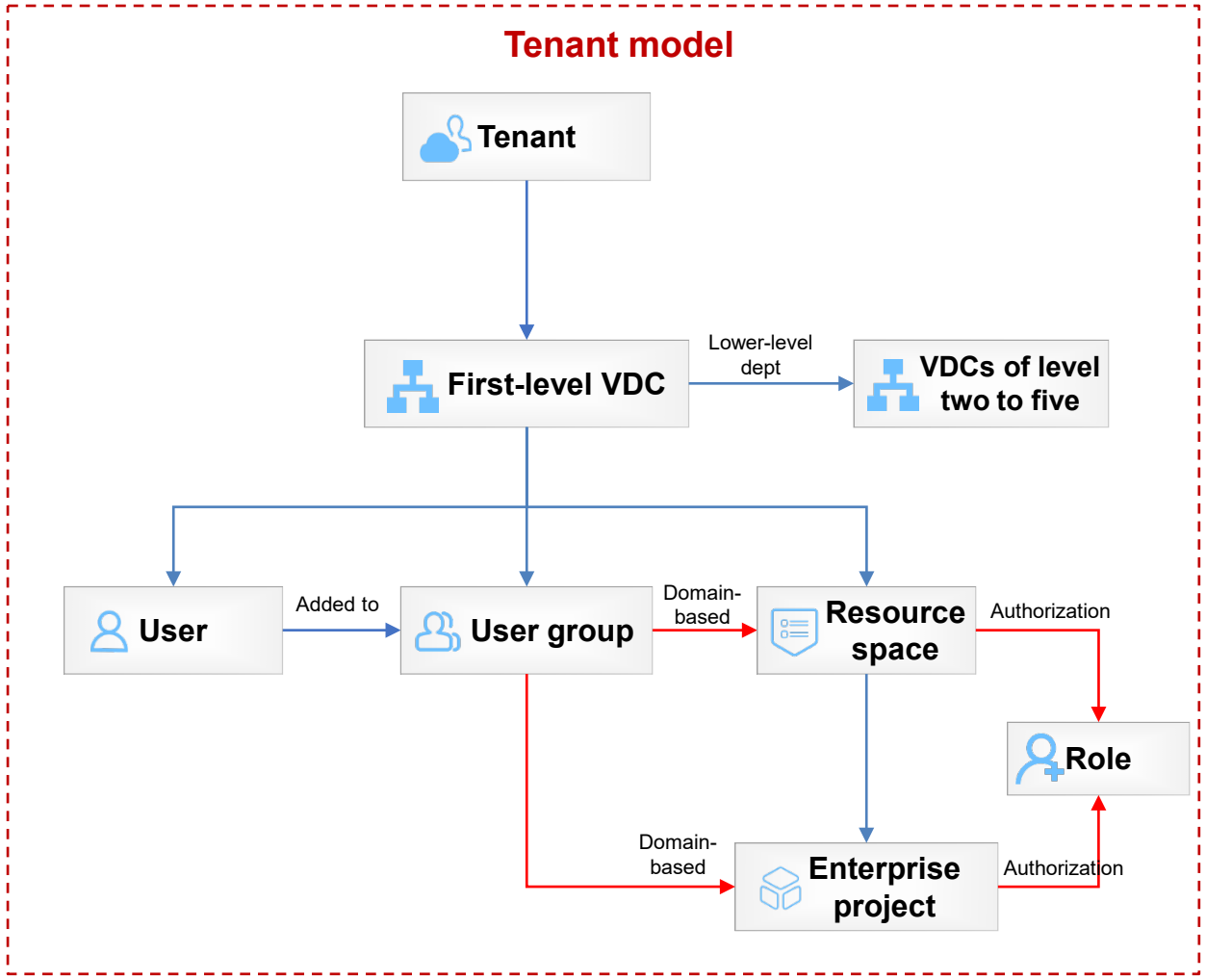
The HCS landing zone design for ABSA contains four parts: Tenant model design, Permission design, Network access design, and cost control design.



Contents

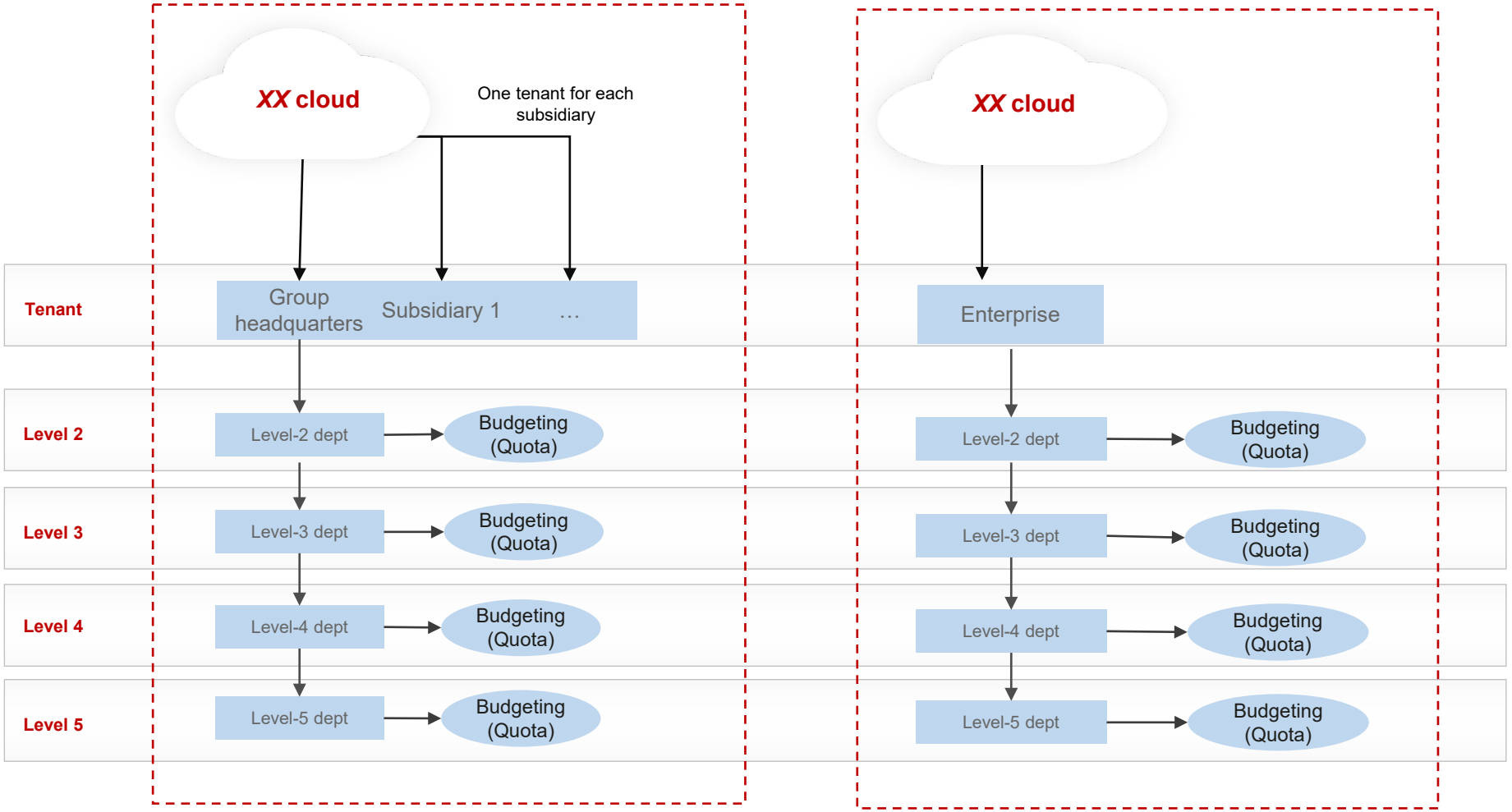
Basic Concepts in Tenant Models

Objects of a tenant model include tenants, resource spaces, enterprise projects, Virtual Data Centers (VDCs), user groups, and users. Enterprises can tailor their tenant models based on actual service scenarios to facilitate information decision-making, task execution, and compliance check.



Object	Description
Tenant	A tenant matches an **enterprise or subsidiary**. Data, operations, and networks are isolated between different tenants.
VDC	VDCs match an enterprise's **departments.** A maximum of five levels of VDCs can be created to adapt to diverse organizational structures.
Resource space	Resource spaces are isolated containers that group **resources for a tenant**. Authorization to a specified resource space grants users access to all resources within it.
Enterprise project	An enterprise project is a unit that **logically divides resources in a resource space**.
User group	Users in a user group inherit all permissions assigned to the user group. After the user group is associated with resource sets, the users have permissions on the resource sets.
User	After a cloud platform user is added to a user group, the user inherits the group's assigned permissions.
Role	A role acts as a label for a specific set of **permissions** defined as required.

Tenant Design Principles

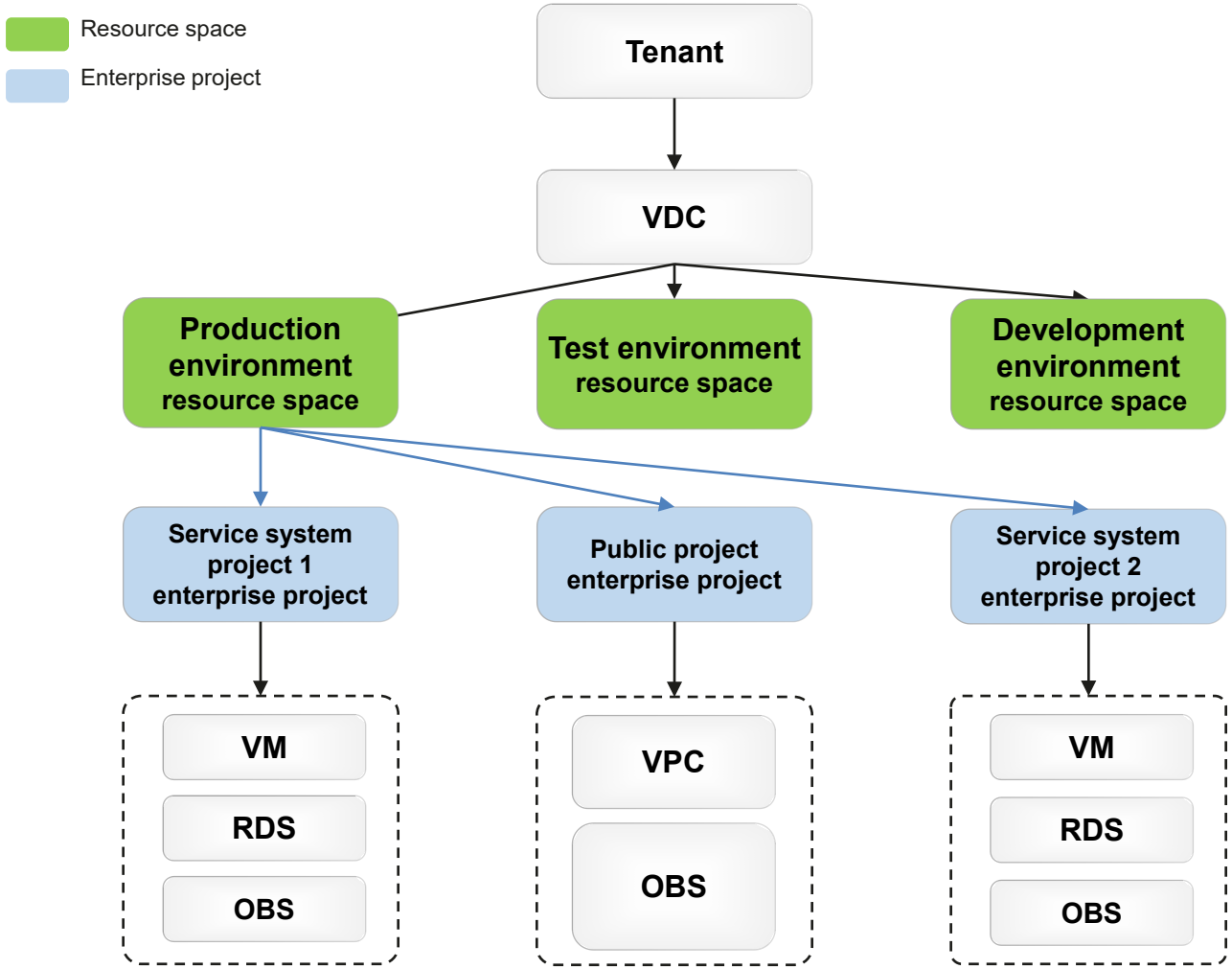


Design principles:

1. Multi-tenant model
   - For a group company, one tenant can be created for the headquarters, and one tenant can be created for each subsidiary.
   - VDCs are created based on cloud departments or functions (production, office, transaction, and public) under the group or its subsidiary.
2. Single-tenant model
   - An enterprise is a tenant.
   - VDCs are created based on cloud departments or functions (production, office, transaction, and public) under the enterprise.

A tenant is an entity that uses resources on the cloud platform and performs independent settlement. A tenant can be an individual, organization, or enterprise.

Resource Space & Enterprise Project Design



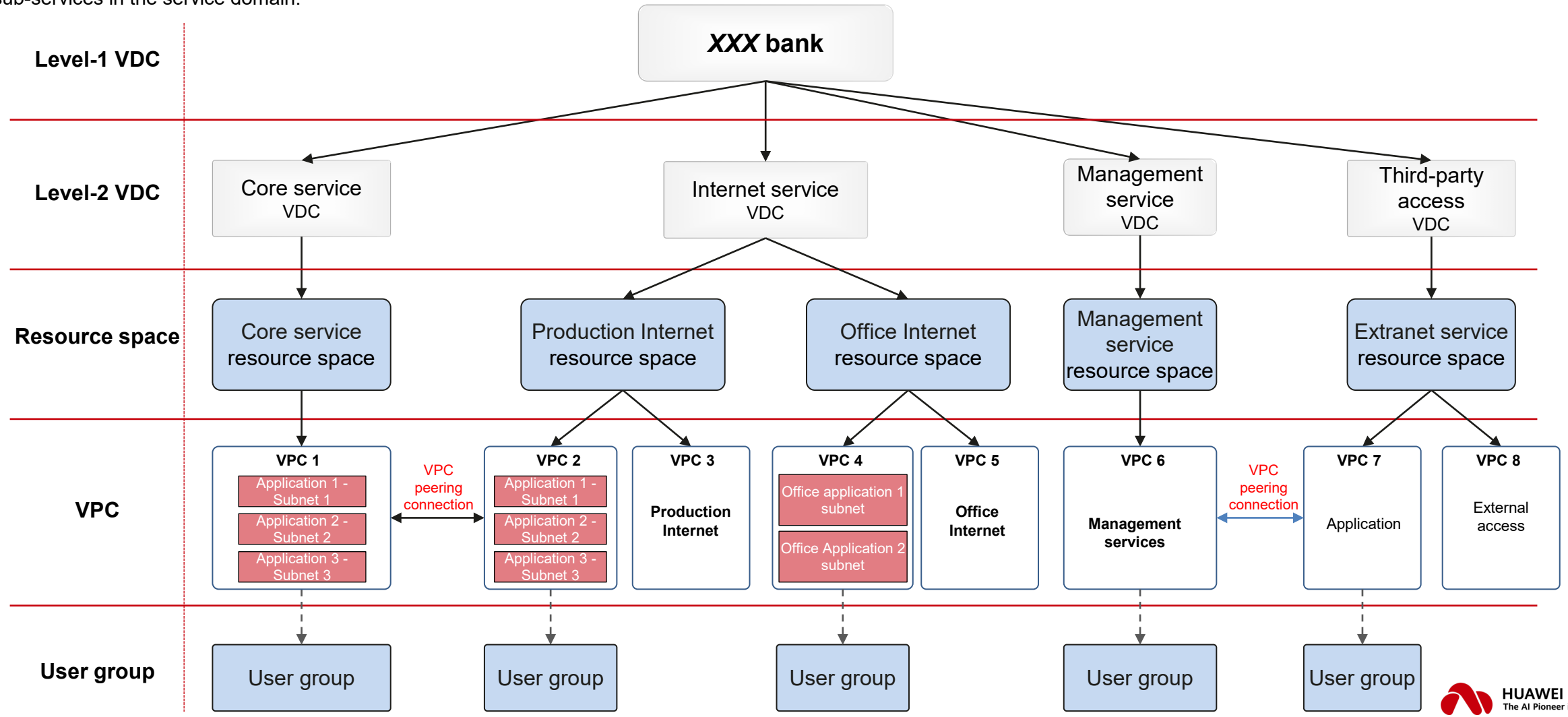
Design principles:

- Enterprise projects: An enterprise project is an authorization domain that can be used to group cloud resources in resource spaces and control access to those resources.
- Rights- and domain-based management:
  - Rights-based management: Roles are assigned to user groups to specify which permissions the user groups have.
  - Domain-based management: The domains where permissions are applied are specified for user groups. There are three domains: tenants, resource spaces, and enterprise projects.
- Suggestions:
  - Public resource sharing: Public projects can be created by department to store public resources, such as OBS buckets, VPCs. The department administrator grants the management permission on the public projects.
  - Application resource isolation: Enterprise projects can be created based on applications to store compute, storage, and other resources required by the applications. Application development and maintenance personnel can grant the project management permission and the read-only permission of public projects to share networks and isolate application resources.

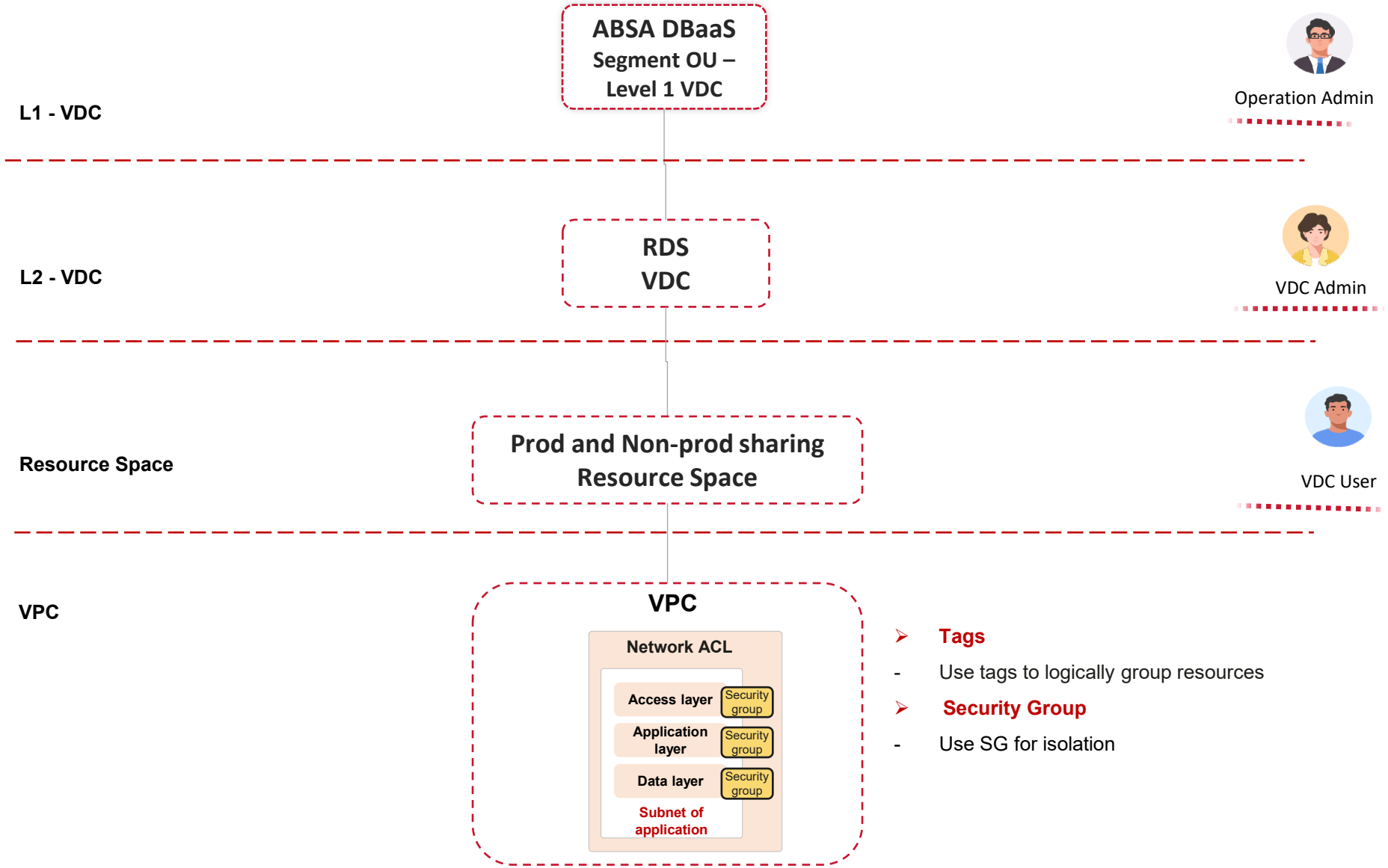
Resource spaces are designed based on environment categories, and enterprise projects are designed based on service systems.

Typical Example: Single-tenant model Designed Based on the Service Domain and Application System

Design a tenant for the bank, create level-2 VDCs in the tenant based on service domains (such as core, Internet, and management services), and allocate resource space based on sub-services in the service domain.

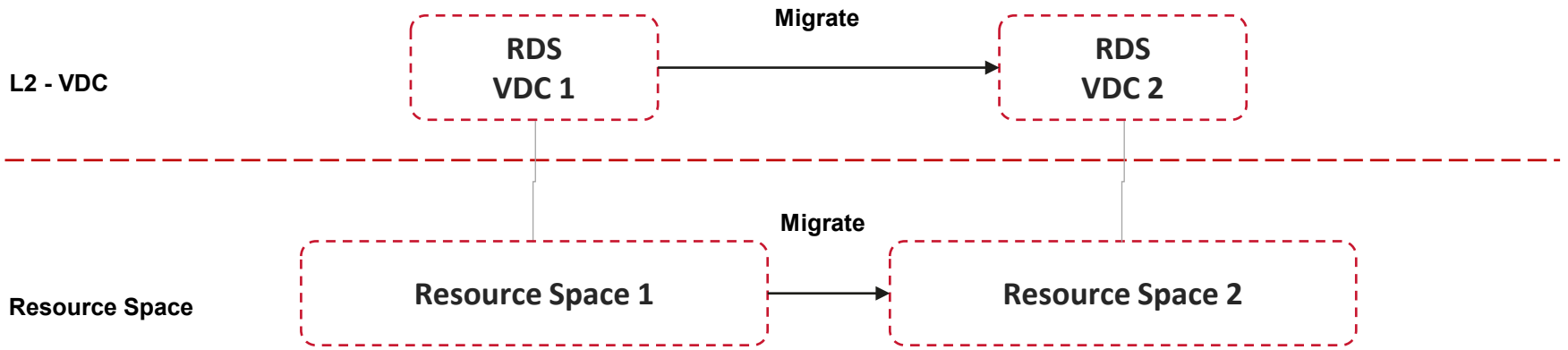


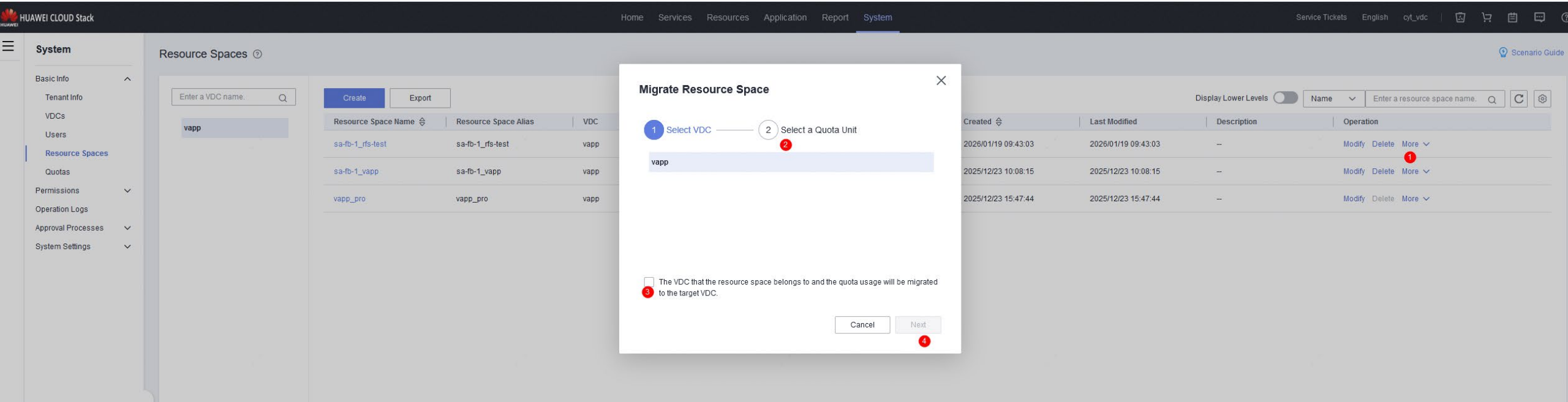
Current Tenant Organization Design-using level-2 VDC



- **Tags**
  - Use tags to logically group resources
- **Security Group**
  - Use SG for isolation

Migrate Resource Space





Take away

Relationships between regions, VDCs, resource spaces, and VPCs:

1. Operation administrators can create first-level VDCs and specify first-level VDC administrators.

2. First-level VDC administrators can create lower-level VDCs and specify administrators for lower-level VDCs. A VDC can be associated with multiple regions, and a service quota can be created for each region.

3. A resource space can belong to only one VDC. You can create resource spaces in a region associated with a VDC.

4. Network resources are a type of service resources, including basic network services such as VPC, EIP, and VPN. You can create multiple VPCs based on the quota for a resource space.

Resource Naming Rules Specified to Improve Resource Maintainability and Team Collaboration Efficiency

1. Naming rules: A name must be easy to understand, easy to identify, and exactly indicate the resource usage and attributes.
   - Readability: A name must be clear and concise, and can express what the resource is and what it is used for.
   - Uniqueness: A resource name must be unique on the cloud platform to avoid conflicts.
   - Consistency: Resources of the same type use the same naming rule for easier identification and management.
   - Scalability: Requirements of different services and teams can be met flexibly.
2. Tenant naming rules: The system provides a global view of tenants, VDCs, resource spaces, enterprise projects, user groups, and roles. You are advised to add labels when designing tenant naming rules.

Business Object	Naming Rule	Example Value	Description
Tenant	• {Enterprise name} • {Cloud brand}	Cloud2 XX cloud	A unique name in the system
VDC	• {Environment type}_vdc • {Organization name}	prod_vdc (VDC for the production zone), dev_vdc (VDC for the testing zone) prod_internal_vdc (intranet services in the production zone), dev_internal_vdc (intranet services in the testing zone)	A unique name in a tenant
Resource space	{Isolation type}_rs	prod_internal_rs (intranet space in the production zone), dev_internal_rs (intranet space in the testing zone)	A unique name in a tenant
Enterprise project	{Application name}_eps	prod_internal_fine_eps (intranet fine application in the production zone) dev_internal_fine_eps (intranet fine application in the testing zone)	A unique name in a tenant
User group	{Management scope}_group	• System user group: network_admin_group, database_admin_group • Application user group: prod_fini_net_admin_group	A unique name in a tenant
Role	{Service scope}_role	• System administrator: network_admin_role • Application administrator: fini_net_admin_role	• System role: A unique name in the system and visible to all tenants • Tenant role: A unique name in a tenant and visible to the current tenant
User	{Enterprise account}	Jenile	A unique name in the system

Resource Naming Rules Specified to Improve Resource Maintainability and Team Collaboration Efficiency

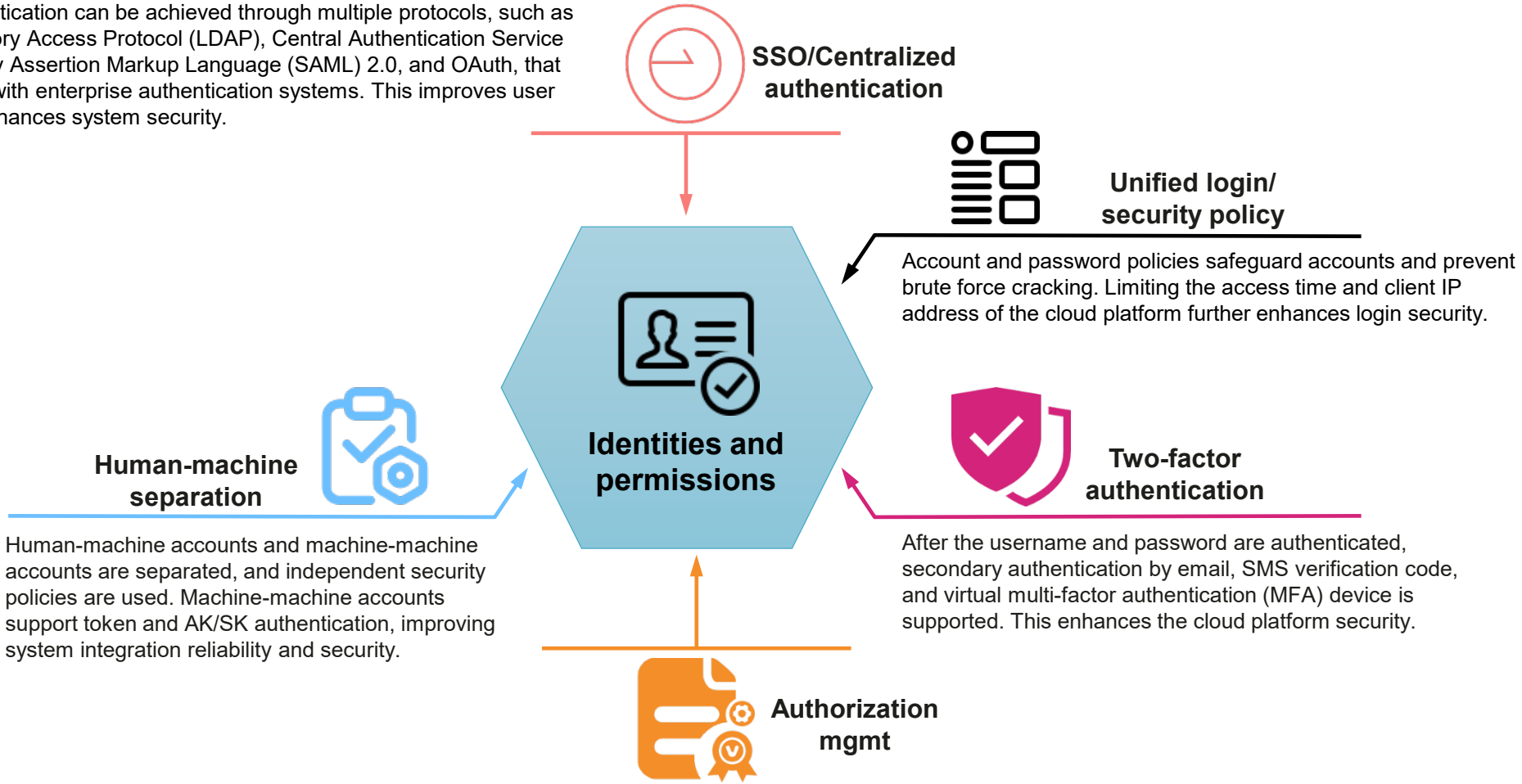
- It is recommended that the cloud resource name be in the *{env}_{resource_type}_{app_name}_{serial_num}* format. Fields can be added or deleted as required.
  - **env**: environment type. Options: **dev** (development), **test** (test), and **prod** (production).
  - **resource_type**: resource type abbreviation, such as **ecs**, **evs**, and **vpc**.
  - **app_name**: name of the application or project to which the resource belongs.
  - **serial_num**: resource sequence number, which can be estimated based on the number of resources required by the application. It is recommended that the value contain four digits and start from 0001.

Business Object	Naming Rule	Example Value	Description
Region	{Cloud brand}-{area}	XXX cloud-SDC, XXX cloud-ADC	Named based on the cloud platform and region
AZ	{name}	Innovation, testing, or database zones	Named by AZ usage. AZ name cannot be modified. The AZ alias can be modified.
Specification	(p|h)(k)AB.C.D	c6.large.2 c6.large.4	**A** specifies the ECS type. For example, **s** indicates a general-purpose ECS, **c** a computing ECS, and **m** a memory-optimized ECS. **B** specifies the type ID. For example, the **1** in **s1** indicates a general-purpose first-generation ECS, and the **2** indicates a general-purpose second-generation ECS. **C** indicates the flavor size, for example, **small**, **medium**, **large**, or **xlarge**. **D** specifies the ratio of vCPUs to memory. For example, value **4** indicates that the ratio of vCPUs to memory is 4.
Disk type	{az_name}-{volume_type}	Database zone-SSD storage pool	Named by disk media type, such as SSD and SATA. The name cannot be changed.
Image	{evn}_{os_version}	SUSE Linux Enterprise Server 15 SP5 64bit	Named by OS version
Environment	{env}_{name}	dev,prod	Name by environment type. Options: **dev** (development), **test** (test), and **prod** (production).
Application	{appname}	welink, wechart	
ECS	{env}_ecs_{appname}_{serial_num}	dev_ecs_welink_001	When you create ECSs in batches, the system automatically adds an incremental number to the end of the custom ECS name, for example, ecs-0001, ecs-0002, and so on.
EVS	{Primary resource name}_volume-{serial_num}	dev_ecs_welink_001_volume-0000 dev_ecs_welink_001_volume-0001	When you create EVS disks in batches, the system automatically adds an incremental number to the end of each disk name, for example, volume-0001 or volume-0002.
VPC	{env}_vpc_{usage}	dev_vpc_internet	
Subnet	{env}_subnet_{usage}	dev_subnet_welink	
RDS cluster	{env}_rds_{appname}	dev_RDS_welink	One application corresponds to one cluster by default. Therefore, there is no need to number the cluster.

Contents

Identities and Permissions: Identity-based Access Control and Permission Authentication Used to Safeguard the Cloud Platform

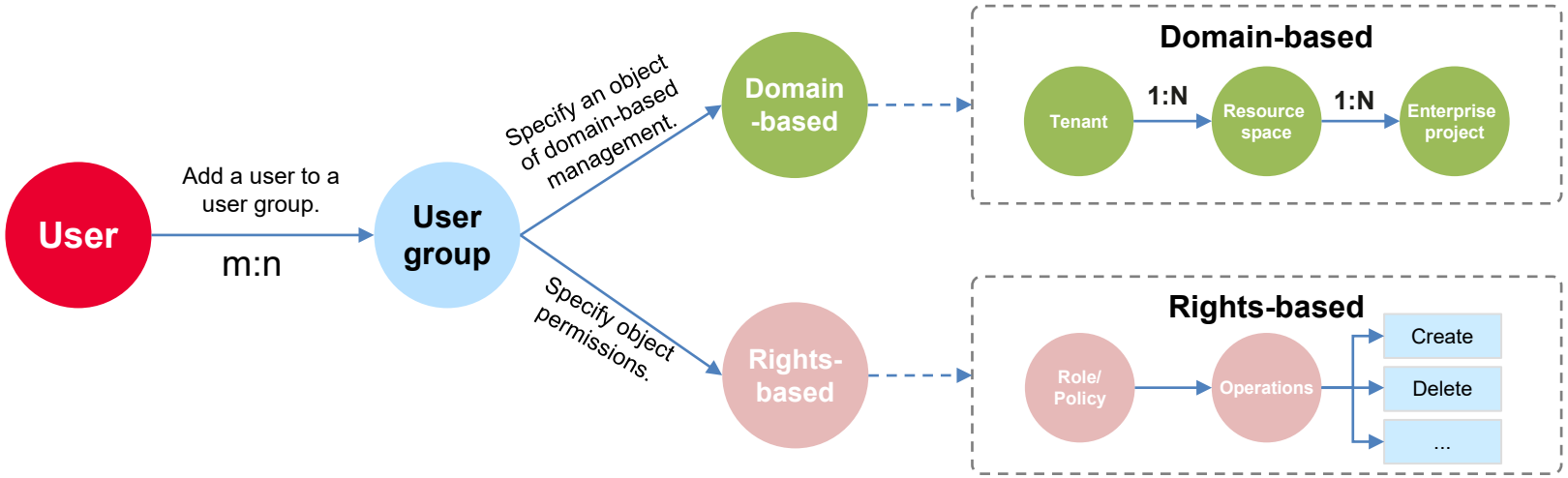
Centralized authentication can be achieved through multiple protocols, such as Lightweight Directory Access Protocol (LDAP), Central Authentication Service (CAS) 2.0, Security Assertion Markup Language (SAML) 2.0, and OAuth, that can be integrated with enterprise authentication systems. This improves user experience and enhances system security.



Authorization Management: Boundary Security Enhanced Through Rights- and Domain-based Management

In rights- and domain-based management, users are authorized based on roles, responsibilities, and managed domains so as to properly control the rights and scope of the operations to be performed. This reduces the probability of security issues caused by misoperations and unauthorized operations. If rights and domains are not divided or are divided improperly, O&M efficiency will be adversely affected, and users may even perform unauthorized operations, causing service interruptions.

- Rights-based management, also known as operation authorization, controls the operations that a user can perform on the system. Unauthorized operations cannot be performed.
- Domain-based management, also known as management authorization, controls the objects that a user can manage on the system. Unauthorized objects cannot be managed.



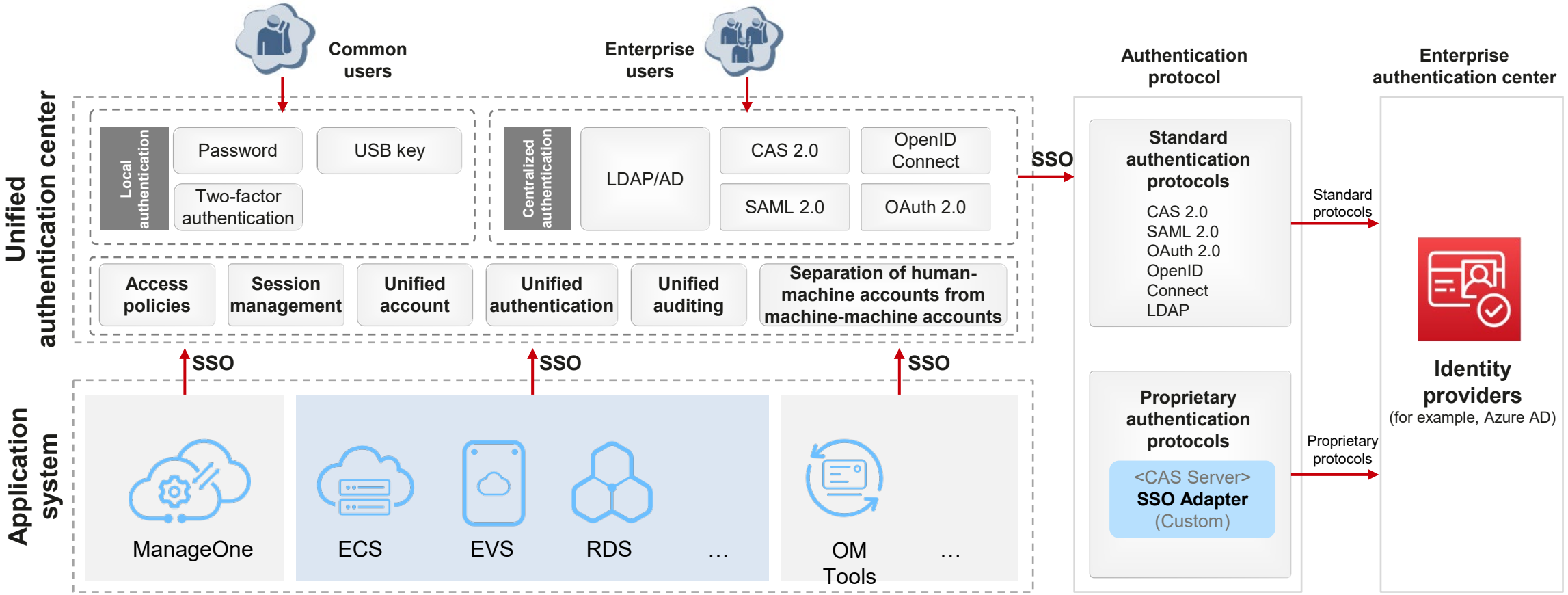
There are default roles in the system to meet the enterprises' basic management requirements. The system also supports custom permissions. Users can create roles and assign specific permissions to them as required. In this way, each employee can access only the required information and functions, ensuring data security and work efficiency.

System Role/Policy Name	Description
Tenant Administrator	Permissions for all services except IAM
Tenant Guest	Read-only permissions for all services except IAM.
* Administrator / * FullAccess	All permissions for the *** service.

Unified Authentication: Unified Access Entry Based on SSO, Improving User Experience and System Security

SSO is an identity authentication solution that allows users to access multiple application systems using one set of identity credentials. Users do not need to log in to each system separately, **eliminating the need for separate accounts, multiple entries, and repeated logins.** SSO has the following advantages:

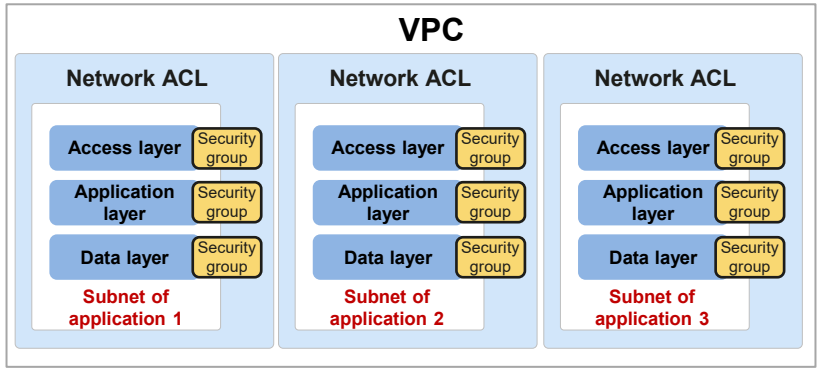
- Improved user experience: Users do not need to repeatedly log in to different applications.
- Enhanced security: User authentication is managed in a centralized manner, reducing the risk of using the same credential in multiple systems and preventing password leakage.
- Streamlined workflows: Users spend less in logging in to different systems and more time in working, boosting efficiency.

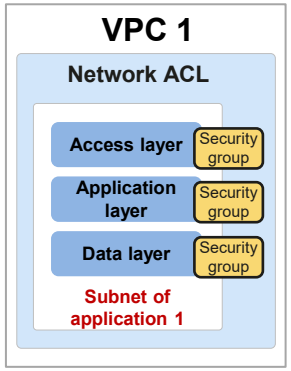


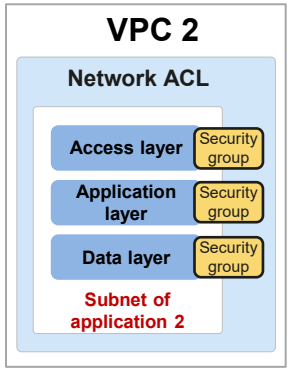
Contents

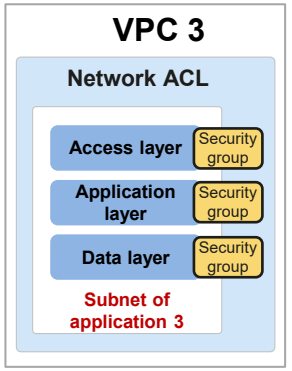
Network Design Principles

1. **Deploy services requiring strict isolation in different VPCs.** By default, different VPCs are isolated from each other, but the subnets in a VPC can communicate with each other.
   - A VPC creates isolated networks based on security zones or service requirements, defining boundaries of the Internet, external network, and internal network.
   - The production, development, and testing environments should be planned in different VPCs.
   - Common services, such as O&M and migration tools, or services that have global impact often reside in independent VPCs.
2. **Deploy intertwined services in the same VPC.** **Applications that are closely related to each other** can be deployed in different subnets of the same VPC to reduce latency. **A subnet is used for only one application** and network ACLs can be used to isolate subnets, which achieves isolation between applications.
3. **Pay attention to the VPC specification baseline**. Up to 500 subnets, 1,200 PMs, and 25,000 IP addresses are supported by a single VPC. If any of these specifications exceeds the baseline, you need to create a new VPC.
4. **Plan CIDR blocks and IP addresses.** Internal IP addresses must be unique and assigned in a unified manner. (**The internal IP addresses cannot conflict with the management CIDR block of the Huawei Cloud Stack platform. Different subnets in the same VPC belong to the same CIDR block.**) It is recommended that three to four times of the current IP addresses be reserved to meet service growth requirements **in the next one to two years**.









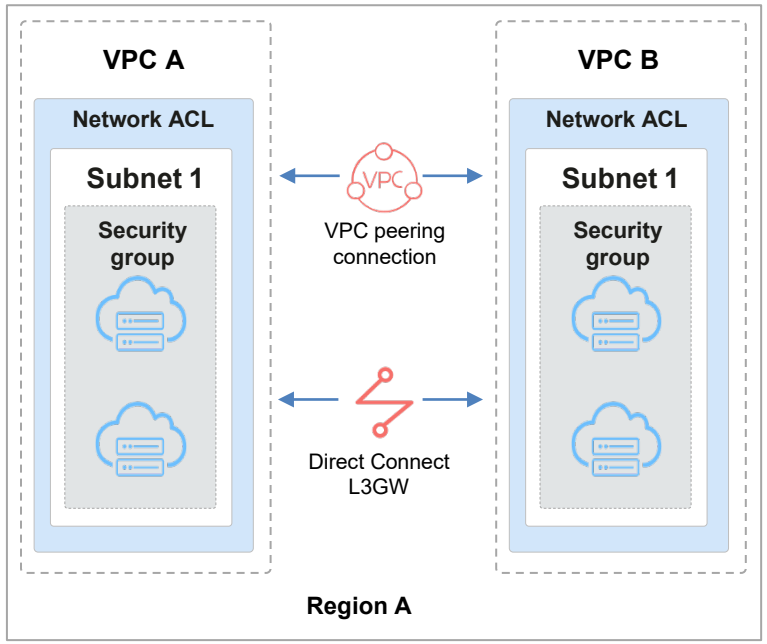
Specification	Value
Maximum number of VPCs in a region	5,000
Maximum number of subnets in a VPC	500
Maximum number of VPC peering connections	200

Solution	Multiple Applications in a VPC	One Application in a VPC
Advantages	• Subnets in the same VPC can communicate with each other by default. This avoids unnecessary VPC peering connections and relieves O&M workload. • **Deploying an application on a subnet** enhances the isolation between different applications. Within the subnet, security groups can be used to isolate logical layers, preventing internal threats. • Network ACLs are configured to manage access policies of different applications and implement access blocklists.	• Deploying an application in a VPC achieves default network isolation and simplifies O&M for more isolation policies. • Applications communicate with each other through VPC peering connections. Network ACLs are used to control mutual access policies, improving network security. • A security group can be configured for an application or based on logical layers of an application to implement internal isolation.

VPC Interconnection Scenarios and Solution Design

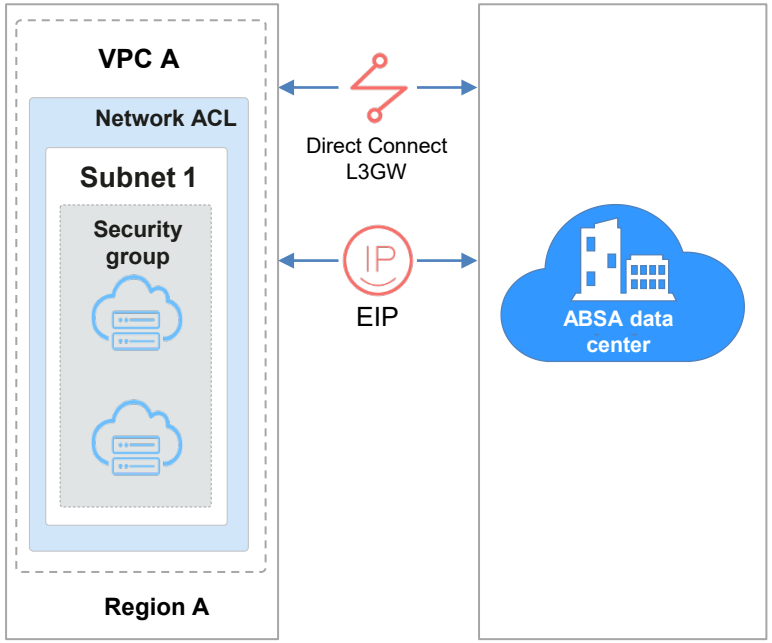
VPCs are region-specific. Cloud resources, such as ECSs, CCE instances, and RDS instances, in a VPC must be in the same region as the VPC. By default, different VPCs are isolated from each other, but the subnets in a VPC can communicate with each other. In a scenario where compute resources in a VPC need to access other resources in another VPC, the VPC peering connection or Layer 3 gateway is used if there is no IP address conflict. If there is an IP address conflict, VPC Endpoint (unidirectional) is used.

Scenario 1: Interconnection between VPCs in the same region



Service	Constraints
Common Function	The CIDR blocks of the local and customer subnets **cannot overlap**.
VPC peering connection	There are a small number of VMs that have no special requirements for performance and latency. The total bandwidth is **less than 80 Gbit/s**.
Direct Connect (ABSA)	• There are a large number of VMs, requiring high performance, low latency, and traffic **greater than 160 Gbit/s**. • Static routes need to be manually added on the switch.

Scenario 2: Interconnection between a VPC and external networks



Service	Constraints
Direct Connect (10.18.240.0/22)	• The CIDR blocks of the local and customer subnets cannot overlap. • High performance, low latency, and traffic **greater than 160 Gbit/s** are required. • Static routes need to be manually added on the switch.
EIP	• The CIDR blocks of the local and customer subnets can overlap. • There are no special requirements for performance and latency. The total bandwidth is **less than 50 Gbit/s**.

Take away

Intra-cloud resource access

- Resources in the same subnet can communicate with each other by default. Access to resources in the same subnet is controlled by security groups.
- Mutual access between subnets. Access between subnets is controlled by ACLs and security groups.
- Inter-VPC resource access is implemented through VPC peering. ACLs, and security groups are used to control access.

Intra-cloud resources access the offline IDC through the L3GW. After the network is connected, intra-cloud resources can access the offline IDC.

Contents

Overall Architecture of Cost Control

As enterprises migrate more and more service systems to the cloud, they tend to focus not only on service stability and reliability, but also on how to improve efficiency while reducing costs. The new focus is not to reduce costs through any one-off action. Instead, enterprises continuously seek optimal solutions to control costs without compromising service efficiency, stability, and security. This also helps enterprises better adapt to market changes and service requirements. Cost control involves the following aspects:

Resource quotas

Multi-dimensional quotas and alarm thresholds can be set for different enterprises and departments by region, resource type, and more. This helps administrators control how to allocate and use resources.

Metering and billing

Metering of multiple resource types and multi-dimensional report statistics are supported. Metering bills support settlement between IT departments and business departments. This helps the IT department transform from a cost center to a value center.

Process approval

Graphical process definition is supported. Approval processes are defined based on enterprise resource compliance requirements. Whether to provision resources is determined based on factors such as the resource pool capacity, remaining quota, and enabling parameters. This ensures the compliance and effectiveness of resource provisioning.

Resource Quota

Quotas are used to manage and control how many resources available to users on the cloud platform. Setting quotas can limit resources usage in specific regions or for specific services. This ensures appropriate resource allocation and utilization. Quotas can be set for various resources, such as CPUs, memory, and storage space. An appropriate quota helps **better meet the requirements of multiple tenants when resources on the cloud platform are limited.** By properly setting quotas, you can effectively allocate resources, avoid resource waste and abuse, and improve resource utilization, thereby ensuring the stability and security of the cloud platform.

Quota indicators of cloud services enabled or disabled based on the quota management policy of the cloud platform

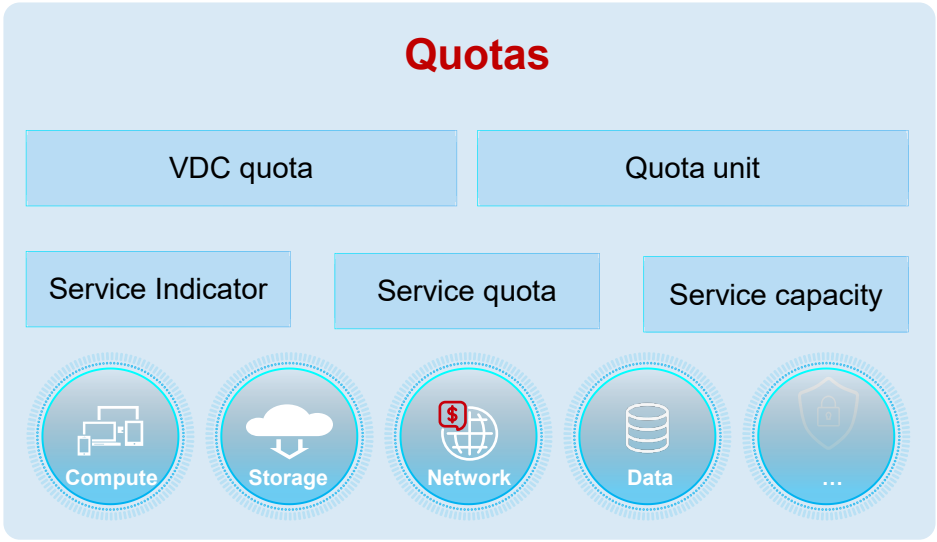
Service indicator

Default quotas that are preset to simplify the allocation process of tenant quotas

Service quota

The maximum quota capacity of the cloud service that is set based on the capacity of hardware resources such as compute, storage, and network resources on the cloud platform

Service capacity



Tenant quota

Resource quotas allocated by the cloud platform administrator to a tenant based on factors such as the customer level and budget.

VDC quota

Resource quotas allocated by a tenant administrator to VDCs based on the department budget

Quota unit

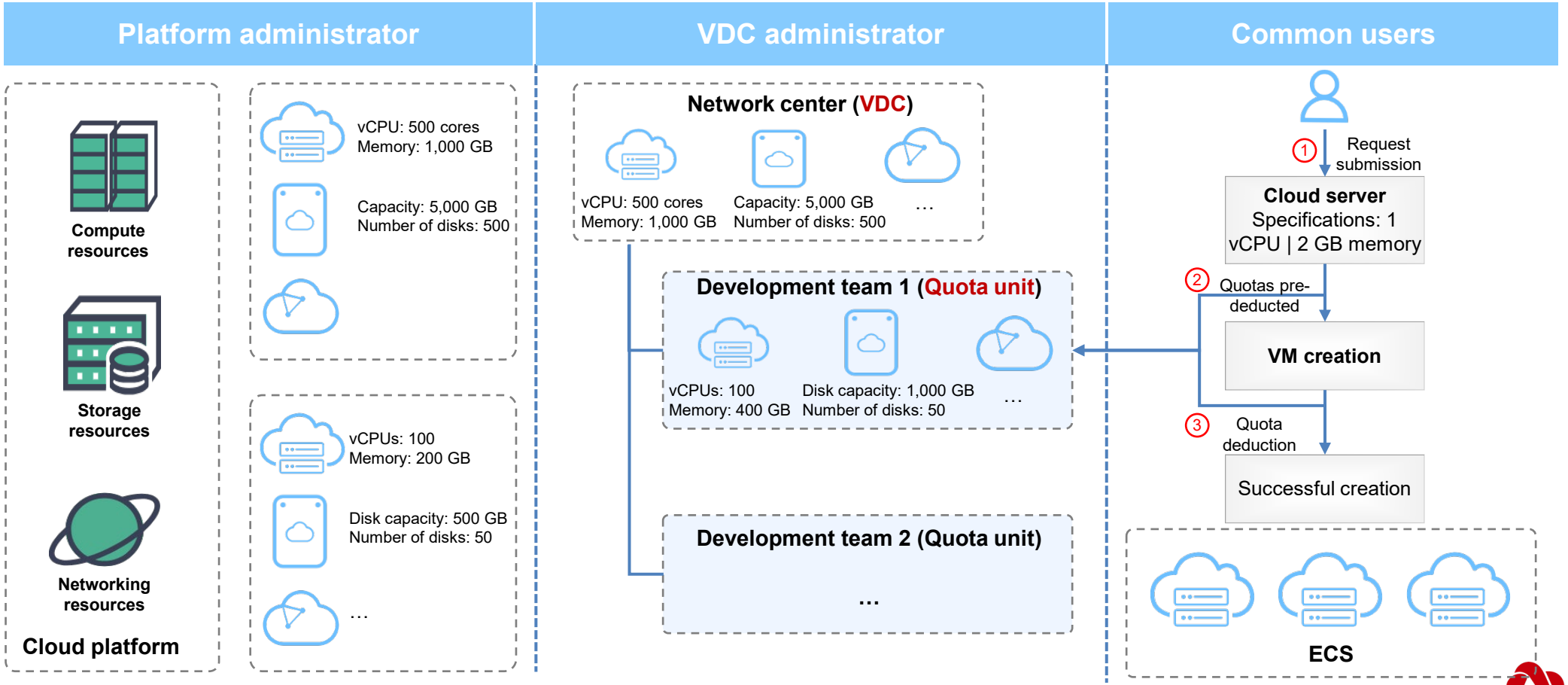
Resource quotas allocated by the department administrator to the quota unit based on the project budget. Cloud resource provisioning consumes quotas in the quota unit.

Service Type	Service Indicator	Quota
ECS	Instances, vCPUs, memory, GPUs, and ECS snapshots	Instances: 10 vCPUs: 100 Memory: 200 GB
EVS	Disk capacity and number of disks	Disk capacity: 1,000 GB; number of disks: 100
VPC	VPC, EIP, network ACLs, load balancers, shared bandwidth, and VPN	
RDS		

Resource Quota Allocation Principles and Deduction Process

Certain users or applications may excessively occupy resources. By setting quotas, you can prevent this situation to ensure that more users can obtain sufficient resources as well. Quota setting involves the following aspects:

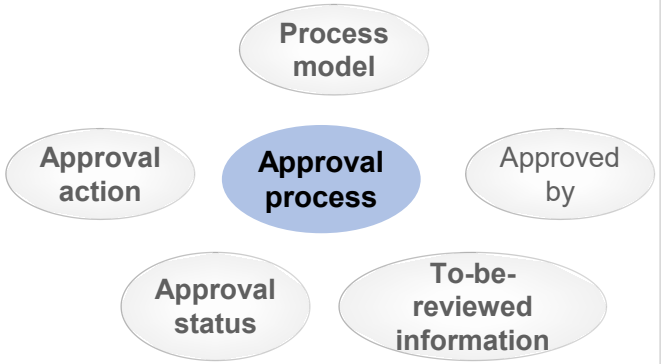
- By resource type: You can set quotas based on the number of resources and resource specifications. For example, 50 ECSs with 1 vCPU and 2 GB memory.
- By hardware type: You can set quotas for SATA disks to 500 GB and SSD disks to 100 GB.
- By application system: For example, a department initiates a project to develop three application systems, and you can calculate the quota based on the application system resource list.
- By the total capacity of the cloud platform: For example, the system reserves 40% of the resource capacity, and the other 60% is allocated to service departments.



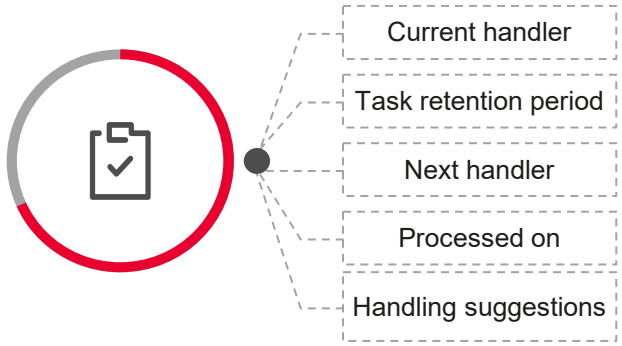
Enterprises' Information Decision-Making Quality Improved and Resource Usage Compliance Ensured By Leveraging the Approval Process

Online approval is a way to improve decision-making quality and efficiency, ensure resource usage compliance, and enhance decision-making transparency, thereby improving internal trust and communication efficiency within an enterprise.

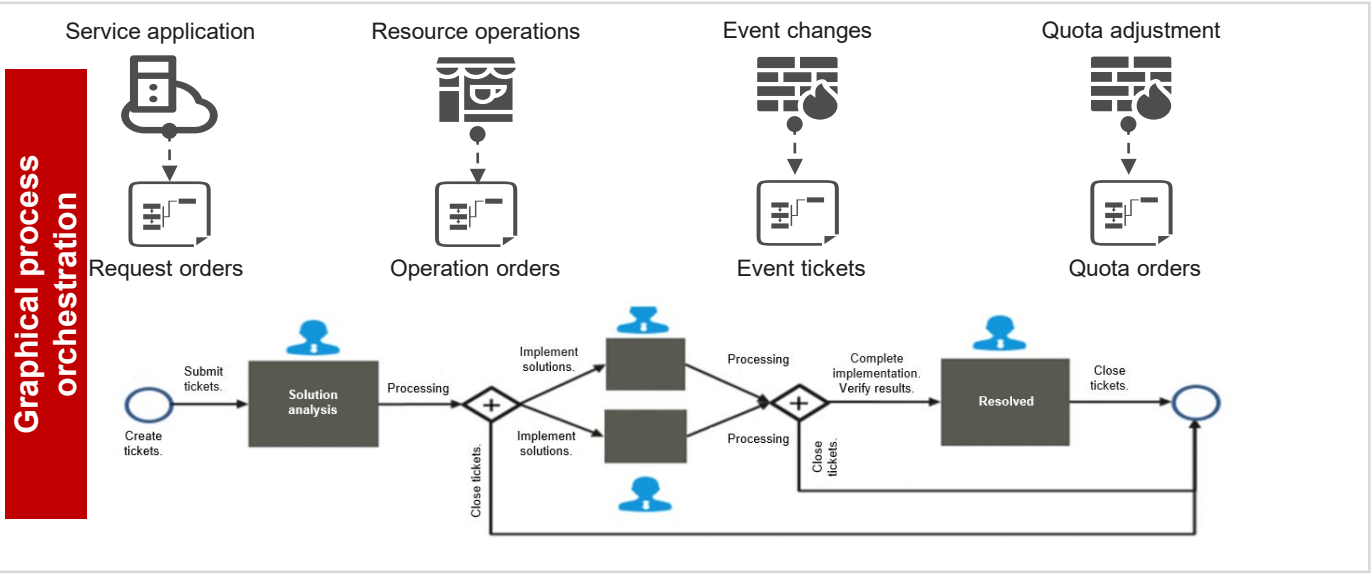
Diverse ticket-related functions



Online, real-time process status



Graphical process orchestration



Challenges

- There are no unified service standards, making cloud use risky.
- Overall operations efficiency of the company is low, resulting in resource waste.
- Customized process control is required to manage different compliance processes.
- Service personnel want to view the process request status and handle issues using online tickets.

Key Capabilities

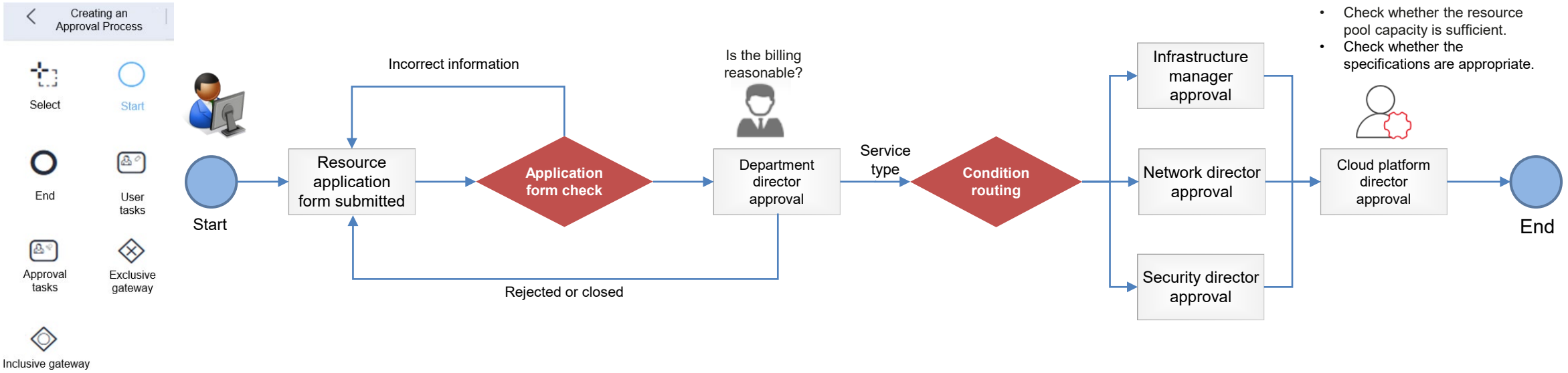
- **Graphical process orchestration**
  - Graphical process orchestration by drag and drop is supported.
  - Approvers can be selected based on policies. After an applicant is entered, the corresponding VDC administrator is automatically matched.
  - Tickets can be handed online, with statuses visible.
- **Diverse form functions**
  - Fields in a process form can be customized.
  - Custom SLA policies can be created to check whether tickets meet requirements.
  - Custom triggers can be defined for emails, SMS notifications, and external interfaces. Administrators define and enable ticket process models as required.
- **Online, real-time process processing**
  - Applicants can learn of ticket statuses, process retention periods, and handling suggestions in a timely manner.

Approval Processes Designed Through Graphical Orchestration, Meeting Enterprise Compliance Management Requirements

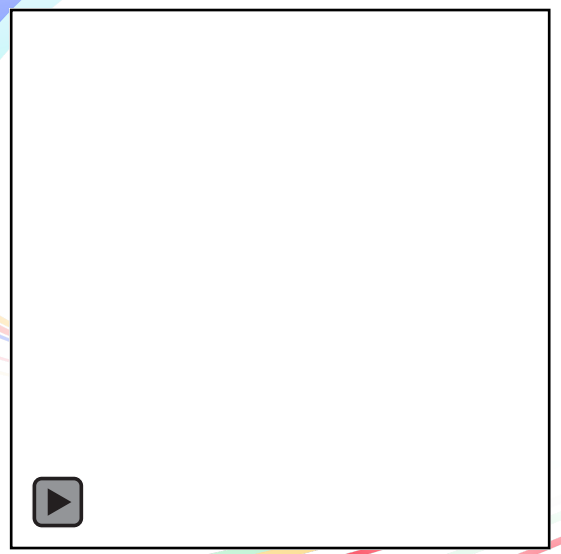
Design principles: Based on the enterprise IT resource management specifications and resource compliance requirements of the cloud platform, design the approval process from multiple dimensions adhering to position responsibilities (such as positions of infrastructure, database, container, and security).

- Determine the service scope that requires online approval, set up corresponding approval teams, and grant different permissions to each team.
- Design and set a specific approval process, and specify the operation mode and precautions for each step.
- Ensure that the designed approval process is reasonable and scientific to avoid messy approval flows.
- Regularly evaluate and optimize online approval processes and forms to better serve enterprise operations.

The graphical process orchestration engine is used to design an approval process online, as shown in the following figure.



Online approval makes operations more efficient, improves enterprise management capabilities and efficiency, and facilitates enterprise digital transformation.



Your story matters absa

HUAWEI CLOUD
The AI Pioneer in Industries