Cloud Computing Basics

Foreword

- The IT sector is a fast-changing industry. Cloud computing has been developing rapidly in recent years and has become the foundation of a wide range of major applications. So, what is cloud computing all about? What are the service models for cloud computing? This course will provide a brief introduction to cloud computing.

Objectives

- On completion of this course, you will be able to:
  - Describe what cloud computing is.
  - Describe the benefits of cloud computing.
  - List services and deployment modes for cloud computing.
  - Understand mainstream cloud computing vendors and representative technologies.

Contents

IT All Around Us

- "IT" is the common term for an entire spectrum of technologies for information processing, including software, hardware, communications, and related services.

A car service company without any cars

Taxis

A hotel without any rooms

Hotels

An instant messaging service company without a network

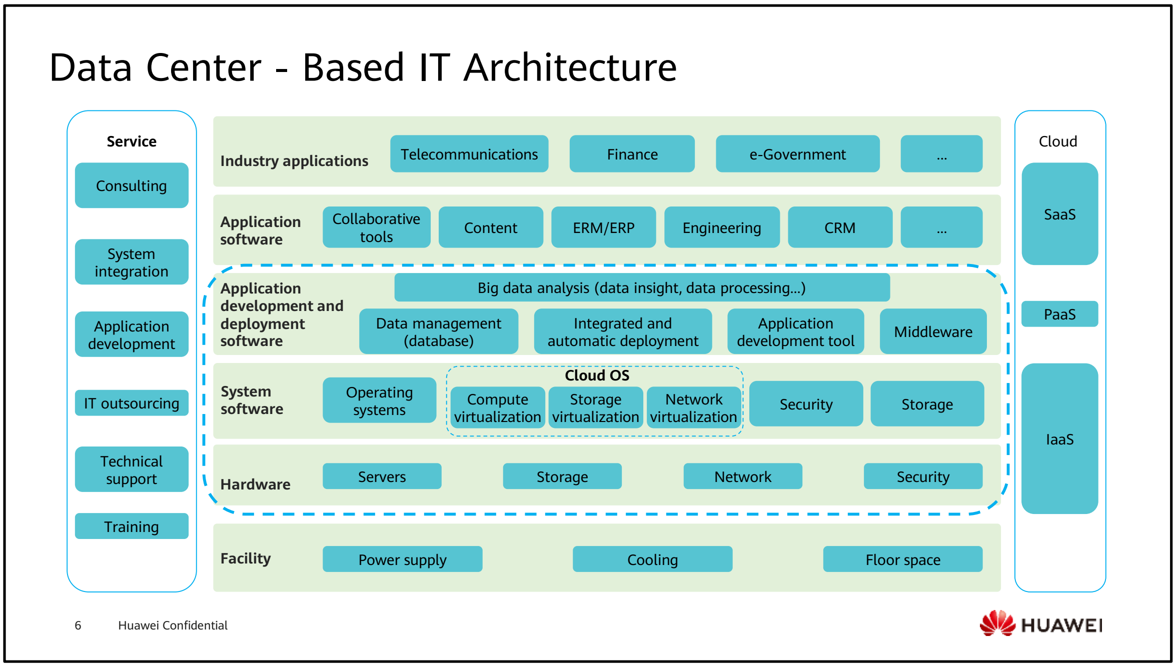
Messaging and calls

A shopping mall without any physical stores

Retail

New technologies and models are changing our lives.

- IT (Information Technology) around us are changing the way we live, for example, taxi hailing software that enables online booking and dispatch of cabs, communications software that enables real-time voice calls over the Internet, and e-malls that provide online shopping experience.
- Taxi hailing: Uber and DiDi
- Hotel: Airbnb
- Messaging and calls: WeChat and Viber
- Retail: Taobao and Amazon

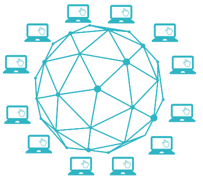


- Traditional IT infrastructure consists of common hardware and software components, including facilities, data centers, servers, network hardware, desktop computers, and enterprise application software solutions.

Contents

The Information Explosion Is Here

- With the proliferation of mobile Internet in today's fully connected era, more devices are getting connected every day. The amount of data being processed has been growing exponentially, which has created unprecedented challenges to traditional ICT infrastructure.

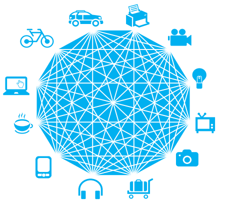


PCs
Computers using
x86 architecture

Windows/Linux

Mobile internet
Mobile phones using
Advanced RISC Machines
(ARM) architecture

Android/iOS



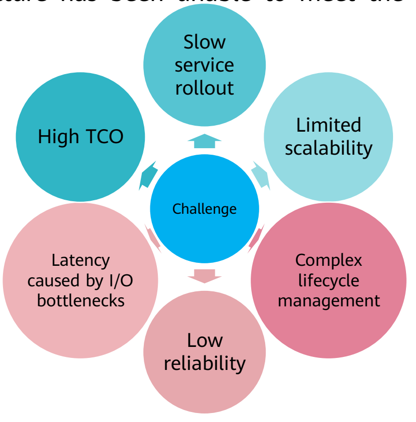
IoT
Terminals running
x86/Arm/DSP/MIPS/FPGA/...

IoT operating systems

- In the PC era, computers are connected to each other through servers. Now, in the mobile era, we can assess the Internet through mobile phones. In the 5G era, all computers, mobile phones, and smart terminals are connected to each other, and we are in the era of Internet of Everything (IoE).
- In the IoE era, the entire industry will compete for ecosystem. From the PC era to the mobile era, and then to the IoE era, the ecosystem changes fast at the beginning, then tends to be relatively stable, and rarely changes when it is stable. In the PC era, a large number of applications run on Windows, Intel chips, and x86 architecture. Then, browsers come with the Internet. In the mobile era, applications run on iOS and Android systems that use the ARM architecture.
- The Internet has gone through two generations and is now ushering in the third generation, the Internet of Everything. Compared with the previous generation, the number of devices and the market scale of each generation increase greatly, presenting future opportunities. As the Intel and Microsoft in the PC era and the ARM and Google in the mobile era, each Internet generation has its leading enterprises who master the industry chain. In the future, those who have a good command of core chips and operating systems will dominate the industry.

Challenges to Traditional IT

- As the Internet has grown, massive volumes traffic, users, and data have been generated. The traditional IT architecture has been unable to meet the demands of fast developing enterprises.



HUAWEI

- The growing popularity of the Internet brings an influx of traffic, users, and data to enterprises. To keep up with the rapidly developing businesses, enterprises need to continuously purchase traditional IT devices. Therefore, the disadvantages of traditional IT devices gradually emerge.
  - Long procurement period slows rollout of new business systems.
  - The centralized architecture has poor scalability and can only increase the processing performance of a single node.
  - Traditional hardware devices are isolated from each other, and their reliability mainly depends on software.
  - Devices and vendors are heterogeneous and hard to manage.
  - The performance of a single device is limited.
  - Low device utilization leads to high total cost of ownership (TCO).

Discussion

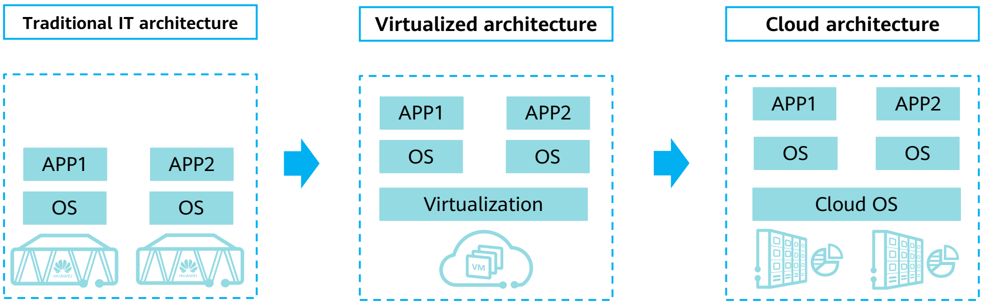
- How can IT enterprises overcome these challenges?

  - **IT infrastructure transformation**
  - **Resource integration and comprehensive utilization**
  - **Business collaboration and continuous optimization**

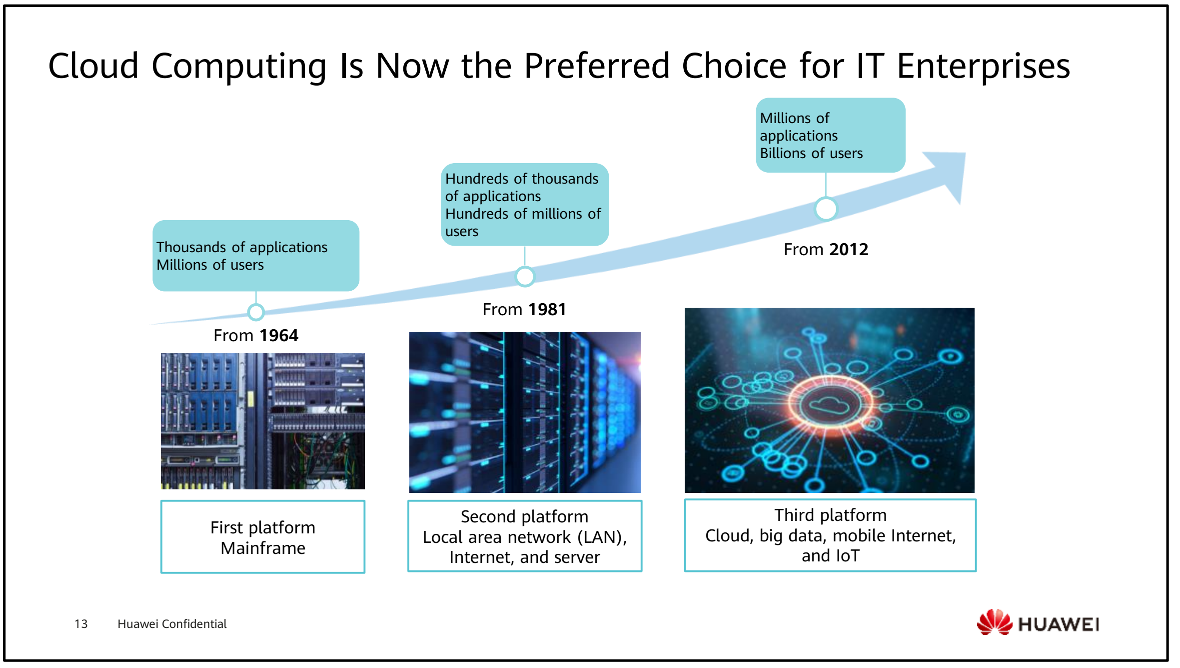
- How do we solve these pain points? Think over advantages of cloud computing that can solve these pain points, so you can have a better understanding of cloud computing.

Contents

Enterprises Are Migrating to the Cloud



- The traditional IT architecture consists of hardware and software, including infrastructure, data centers, servers, network hardware, desktop computers, and enterprise application software solutions. This architecture requires more power, physical space, and money and is often installed locally for enterprise or private use only.
- With the virtualization technology, computer components can run on the virtual environment rather than the physical environment. Virtualization enables maximum utilization of the physical hardware and simplifies software reconfiguration.
- Enterprise data centers are transformed from resource silos to resource pooling, from centralized architecture to distributed architecture, from dedicated hardware to software-defined storage (SDS) mode, from manual handling to self-service and automatic service, and from distributed statistics to unified metering. These are the key features of cloud migration of enterprise data centers.



- In 2015, the third platform gained prominence over the second platform.
- The third platform accounts for one-third of the global IT spending and 100% of IT spending growth.
- Cloud computing has changed the business and construction mode of the IT industry. Big data assists enterprises in exploring business benefits and promoting the construction of the second data plane.

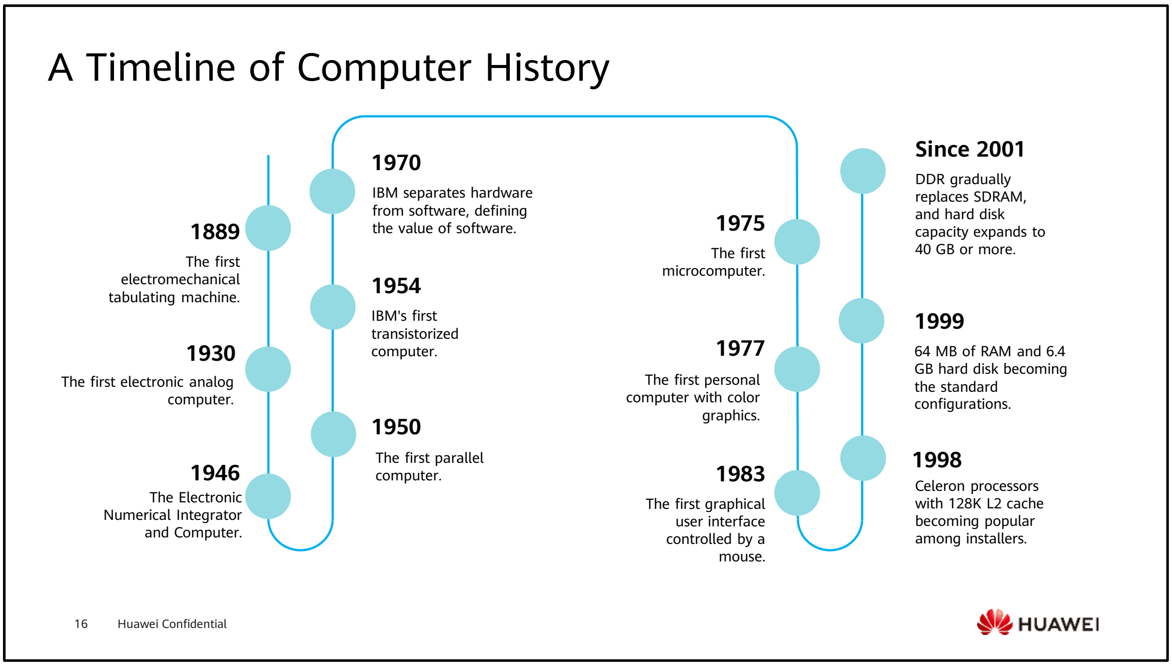
Contents

- As what we have learnt from the previous slides, the third platform built on cloud computing has become the mainstream of the IT industry. Computer and virtualization technologies are the foundation of the third platform. Before we get into cloud computing, let's take a quick look at the evolution of computer and virtualization technologies.

What Is a Computer?

- A computer is a high-speed electronic device capable of performing numerical and logical calculations. It automatically stores and processes data according to a set of programming instructions given to it.

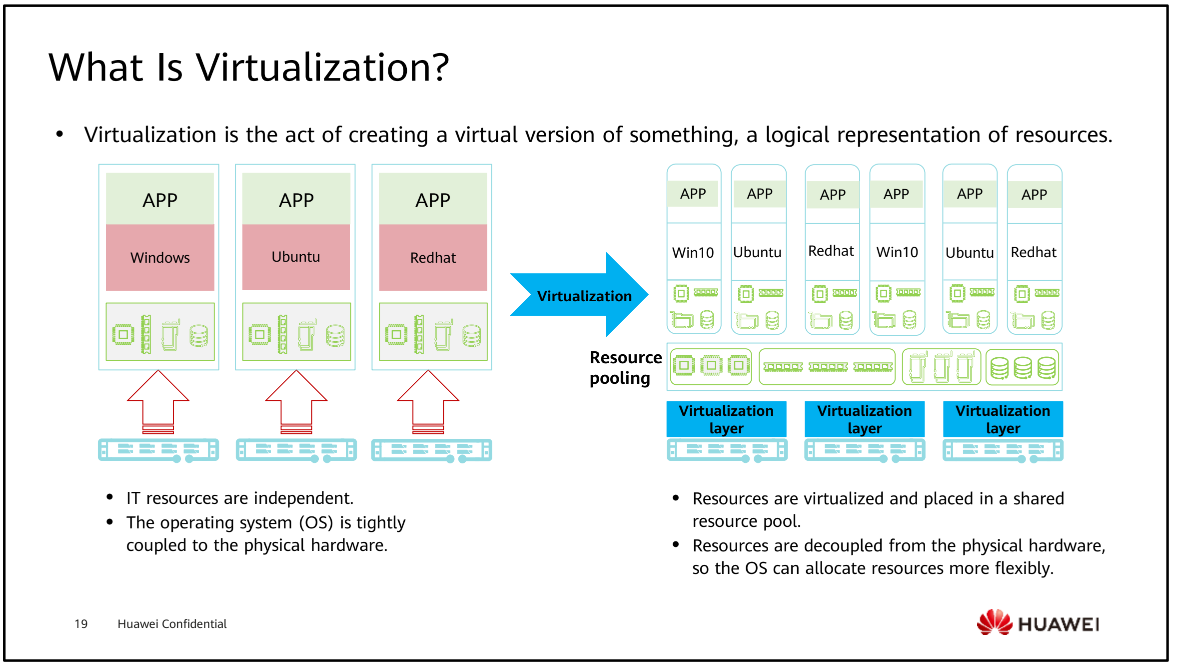
- When it comes to computers, we immediately think of desktops, laptops, and servers. Actually, storage devices, network devices, and security devices in a data center are all computer devices.



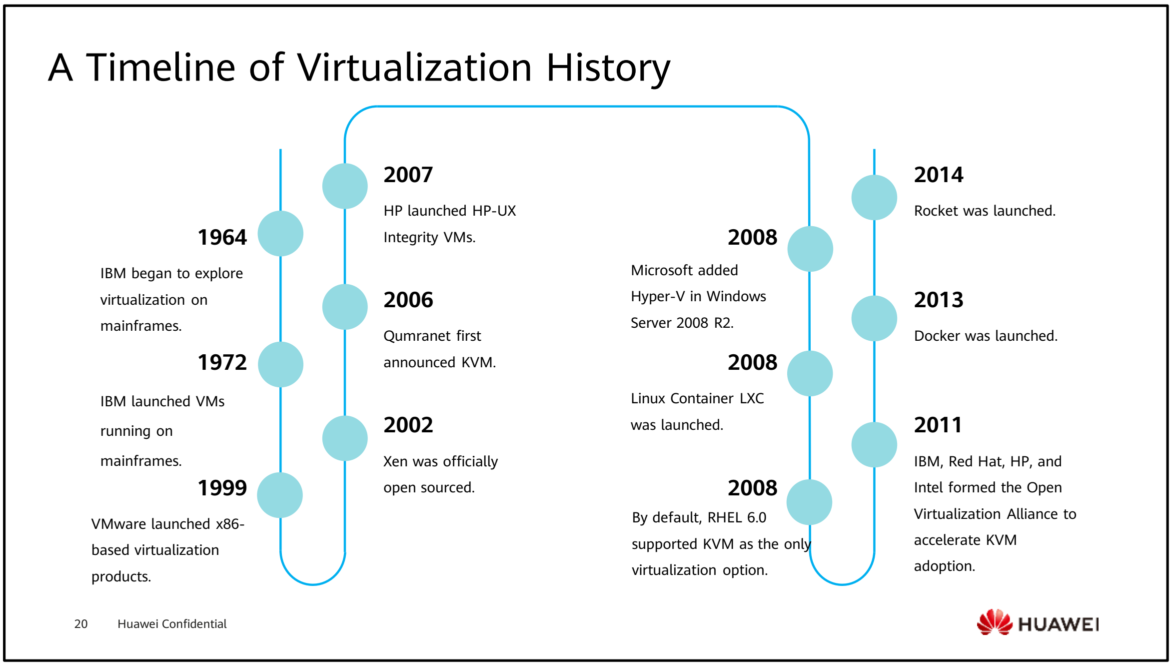
- Computing tools progressed from simple to complex and from low to high level, such as knotting to abacus and calipers, and then mechanical computers. They played historical roles in different periods and also inspired the development of modern electronic computers.
- In 1889, American scientist Herman Hollerith developed an electromechanical tabulating machine for storing accounting data.
- In 1930, American scientist Vannevar Bush built the world's first analog computer with some digital components.
- In 1946, the U.S. military customized the world's first electronic computer, the Electronic Numerical Integrator and Computer.
- In 1950, the first parallel computer was invented, using von Neumann architecture: binary format and stored programs.
- In 1954, IBM made the first transistorized computer, using floating-point arithmetic for improved computing capabilities.
- In 1970, IBM System/370 was announced by IBM. It replaces magnetic core storage with large-scale integrated circuits, uses small-scale integrated circuits as logical components, and applies virtual memory technology to separate hardware from software, thereby defining the value of software.

- In 1975, MITS developed the world's first microcomputer.
- In 1977, the first personal computer with color graphics was invented.
- In 1998, Celeron processors with 128K L2 cache became popular among installers, and 64MB of RAM and 15-inch displays became standard configurations.
- In 1999, Pentium III CPUs became a selling point for some computer manufacturers. The 64MB of RAM and 6.4GB hard disk became standard configurations.
- Since 2001, Pentium 4 CPUs and Pentium 4 Celeron CPUs have been the standard configurations for computers. DDR has gradually replaced SDRAM as the common type of memory. In addition, 17-inch CRT or 15-inch LCD displays have been the preferred choice for customers. The capacity of hard disks has gradually expanded to 40GB or more.

Contents



- Virtualization is the fundamental technology that powers cloud computing. Simply speaking, virtualization allows multiple virtual machines (VMs) to run on a physical server. The VMs share the CPU, memory, and I/O hardware resources on the physical server, but they are logically isolated from each other.
- In computer science, virtualization creates an abstraction layer over computer hardware for resource simulation, isolation, and sharing by one or multiple operating systems.
- In essence, virtualization is a process that a lower-layer software module provides a virtual software or hardware interface that is completely consistent with what an upper-layer software module requires so that the upper-layer software module can directly run in the virtual environment. Virtualization abstracts a resource into one or more parts by means of space division, time division, and simulation.
- Virtualization creates an isolation layer to separate hardware from upper-layer applications so that multiple logical applications can run on one hardware.



- In 1964, "Big Blue" IBM began experimenting with virtualization on mainframes.
- In 1972, IBM officially named System370's time-sharing system virtual machine.
- In 1999, VMware introduced the first virtualization product to run on the x86 architecture.
- In 2002, Xen was officially open source, and versions 1.0 and 2.0 were released. After that, Xen began to be integrated as a virtualization solution with Linux distributions such as Red Hat, Novell, and Sun. In 2004, Intel engineers began adding hardware virtualization support to Xen to prepare the necessary software for the upcoming new processors. Thanks to their efforts, Xen 3.0, released in 2005, officially supports Intel's VT technology and IA64 architecture. Therefore, Xen VMs can run operating systems without modification.
- In October 2006, Qumranet officially announced the birth of KVM after completing the optimization of basic functions, live migration, and major functions and performance. In October of the same year, the source code of the KVM module was officially incorporated into the Linux Kernel as a part of the kernel source code.
- Between 2006 and 2010, traditional IT vendors launched their own products in virtualization. In 2007, HP introduced Integrity virtual machines and Microsoft added Hyper-V to Windows Server 2008 R2. In November 2010, Red Hat introduced RHEL 6, a new enterprise edition of Linux, which integrates the latest KVM virtual machines and replaces Xen integrated in the RHEL 5.x series.
- In 2011, IBM, Red Hat, HP, and Intel established the Open Virtualization Alliance

to accelerate KVM promotion.

- In 2013, the Docker container project was launched. Docker introduces a complete ecosystem related to container management. These include an efficient hierarchical container image model, a set of global and local container registries, a simplified REST API, a command-line interface, and more. Docker has also built a container cluster management solution called Docker Swarm. Launched in 2014, Rocket was originally developed by CoreOS to address some of the flaws in Docker. CoreOS aims to surpass Docker in its ability to meet security and production requirements. Rocket builds on the App Container specification and makes it a more open standard.

Contents

Definition of Cloud Computing

- The National Institute of Standards and Technology (NIST) defines cloud computing as follows:
  - Cloud computing is a model for enabling **ubiquitous, convenient, on-demand** network access to **a shared pool** of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be **rapidly provisioned and released with minimal** management effort or interaction with service providers.
- Wikipedia:
  - Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

HUAWEI

- Key points:
  - Cloud computing is a model rather than a technology.
  - With cloud computing, users can access IT resources such as networks, servers, storage, applications, and services easily.
  - Simply put, the cloud is a metaphor for the Internet. It is an abstraction of the Internet and the infrastructure underpinning the Internet. Computing refers to computing services provided by a sufficiently powerful computer, including a range of functionalities, resources, and storage. Cloud computing can be understood as the delivery of on-demand, measured computing services over the Internet.

Cloud Services and Applications All Around Us (Personal)

Cloud albums

Cloud music

Cloud video

Cloud Docs

What other cloud services and applications are parts of our lives?

- What are the data sources of cloud computing in daily life?
  - Cloud album, such as Baidu Cloud and iCloud Shared Album
  - Cloud music, such as NetEase Cloud Music, Kugou Music, Kuwo Music, and Xiami Music
  - Cloud video, such as Baidu Cloud and Tencent Cloud Video
  - Cloud documents, such as Youdao Note, and Shimo document
- From the applications we use in our life, we can see that cloud computing makes our life more convenient. Enterprises also use cloud computing to provide better products for better user experience.

Cloud Services and Applications All Around Us (Enterprise)

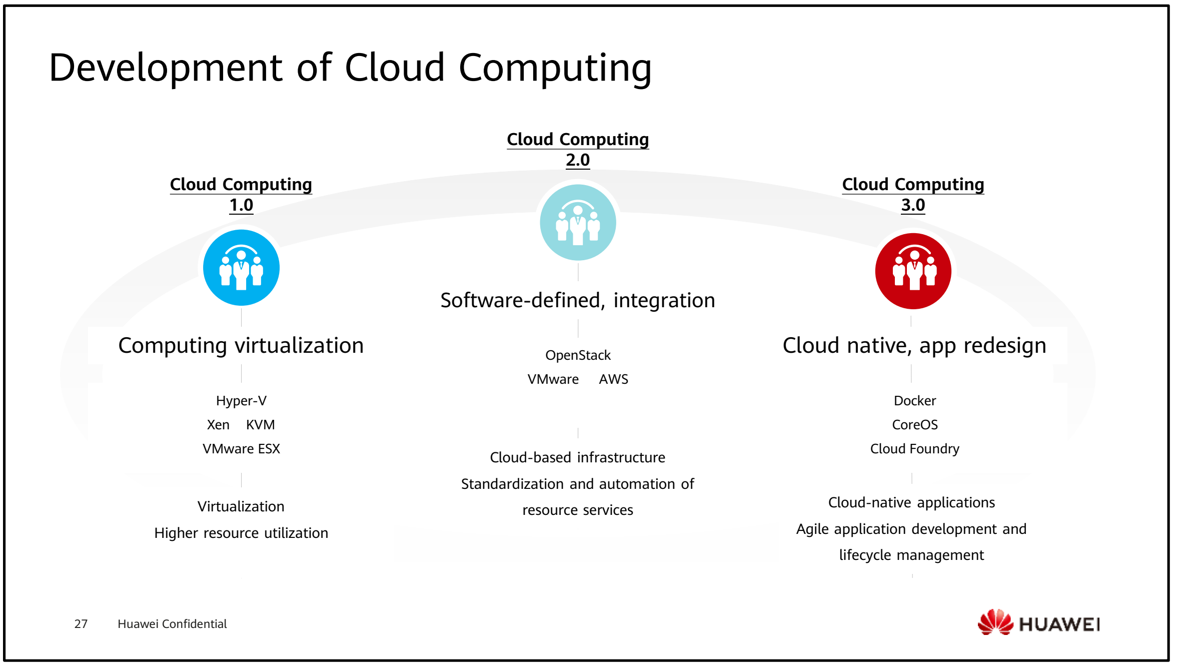
- Huawei Cloud Meeting provides an all-scenario, device-cloud synergy videoconferencing solution for intelligent communication and collaboration on different terminals, in different regions, and with collaborators in other companies.

Videoconferencing

Livestreaming

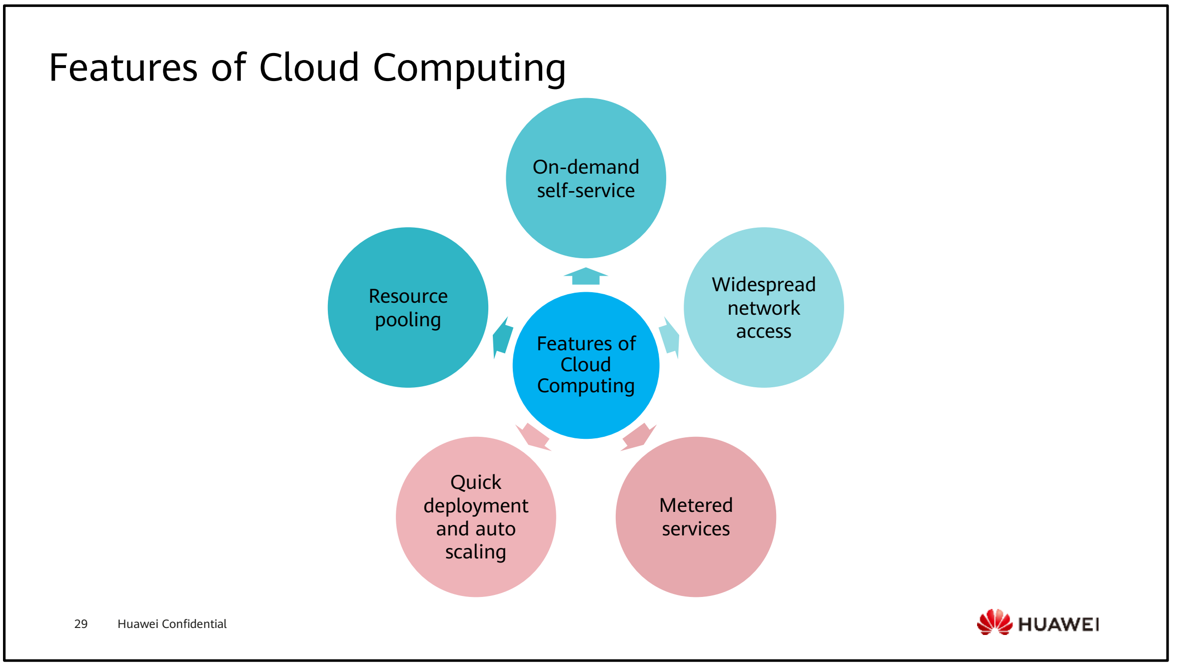
- Driven by the requirements of the government, transportation, electric power, medical care, education, finance, and military industries and enterprises, the video conferencing market in China has an average annual growth beyond 20%. Currently, only less than 5% of enterprises in China have video conference rooms, and more enterprises are aware of the importance of efficient collaboration. Therefore, the video conferencing system has become indispensable for efficient office work.
- Huawei Cloud Meeting can be used by enterprise office, telemedicine, smart education, and enterprise organization construction.

Contents



- With the rapid development and breakthrough of cloud computing technologies in various industries, the application and value exploration of cloud computing have penetrated into all aspects of enterprise IT informatization and telecom network transformation. Industries and enterprises continue to deepen the degree of enterprise IT cloudification based on their business status, competition forms, and informatization transformation, and move from one milestone to the next.
- Since the birth of the cloud computing concept, the enterprise IT architecture has evolved from the traditional non-cloud architecture to the target cloud-based architecture. The evolution can be summarized as follows:
  - Cloud Computing 1.0: IT infrastructure resource virtualization phase for data center administrators.
  - Cloud Computing 2.0: provides resource servitization and management automation for infrastructure cloud tenants and users.
  - Cloud Computing 3.0: A distributed microservice-based enterprise application architecture, Internet-based reconstruction of enterprise data architecture, and big data intelligence phase for enterprise IT application developers and management maintainers.

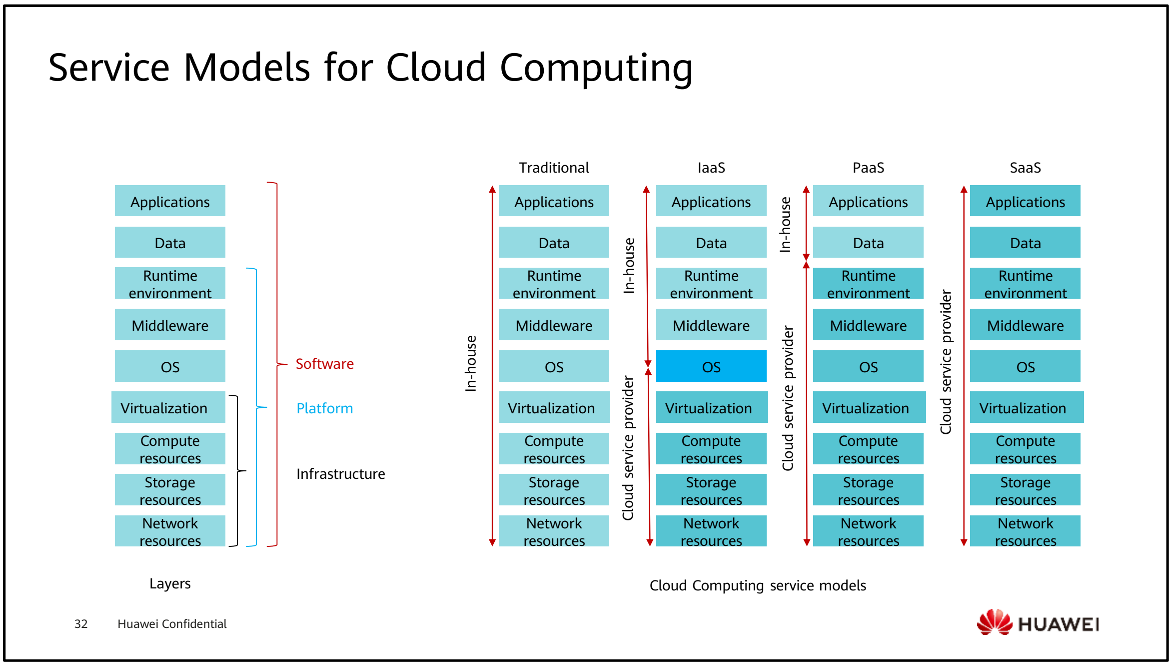
Contents



- Cloud computing integrates hardware resources in software mode and then allocates them to applications for improved resource utilization. Cloud computing helps you run your infrastructure more efficiently, and scale as your business needs change. You can build a cloud data center and use automatic scheduling technology for more unified data storage. In this way, you can use data assets more effectively to save energy, reduce emission, and make maintenance easier. It helps you lower costs and improve efficiency.
- Five main features:
  - On-demand self-service: Consumers can deploy processing capabilities on demand, such as server running time and network storage, and do not need to communicate with each service provider.
  - Widespread network access: Users can access various services over the Internet via different clients, such as mobile phones, laptops, and tablets.
  - Resource pooling: The computing resources are pooled and provisioned in a multi-tenant model. In addition, physical and virtual resources are dynamically assigned based on user demand. Users do not need to know or control the exact location of resources, including storage, processors, memory, network bandwidth, and virtual machines (VMs).

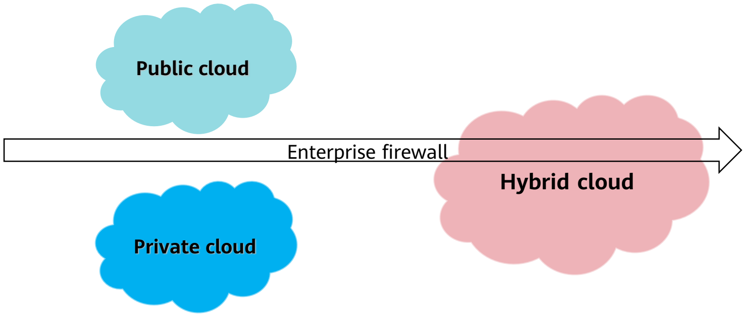
- Quick deployment and auto scaling: Computing resources can be rapidly and elastically provisioned, expanded, and released. A user can rent unlimited resources at any time.
- Metered services: Users pay as per use of cloud server resources, such as CPU, memory, storage, and network bandwidth. You can pay by hour, or you can also buy yearly or monthly package.

Contents



- Infrastructure as a Service (IaaS): The cloud platform provides infrastructure (such as servers, storage devices, networks, and virtual resources) and maintains related resources. Users only need focus on systems and applications.
- Generally, cloud service providers do not provide operating systems for users in IaaS. However, if a user applies for an ECS on the cloud computing platform, the user cannot directly use the ECS without providing an operating system. Therefore, in actual scenarios, the operating system is provided by binding with the IaaS. Therefore, the demarcation point between the self-operated part and the cloud service provider part in the IaaS diagram is the operating system.
- Platform as a Service (PaaS): The cloud platform provides infrastructure (such as servers, storage devices, networks, and virtual resources) and application deployment environment (such as the operating system, middleware, and software running environment) and maintains related resources. Users only need to focus on applications and data.
- Software as a Service (SaaS): The cloud platform provides all resources, services, and maintenance. Users only need to use applications.
- Compared with the conventional IT entire-process and all-device procurement mode, the cloud service-oriented mode provides IT devices as services that allow customers to select on demand, which has more advantages in flexibility, and low cost.

Deployment Models for Cloud Computing



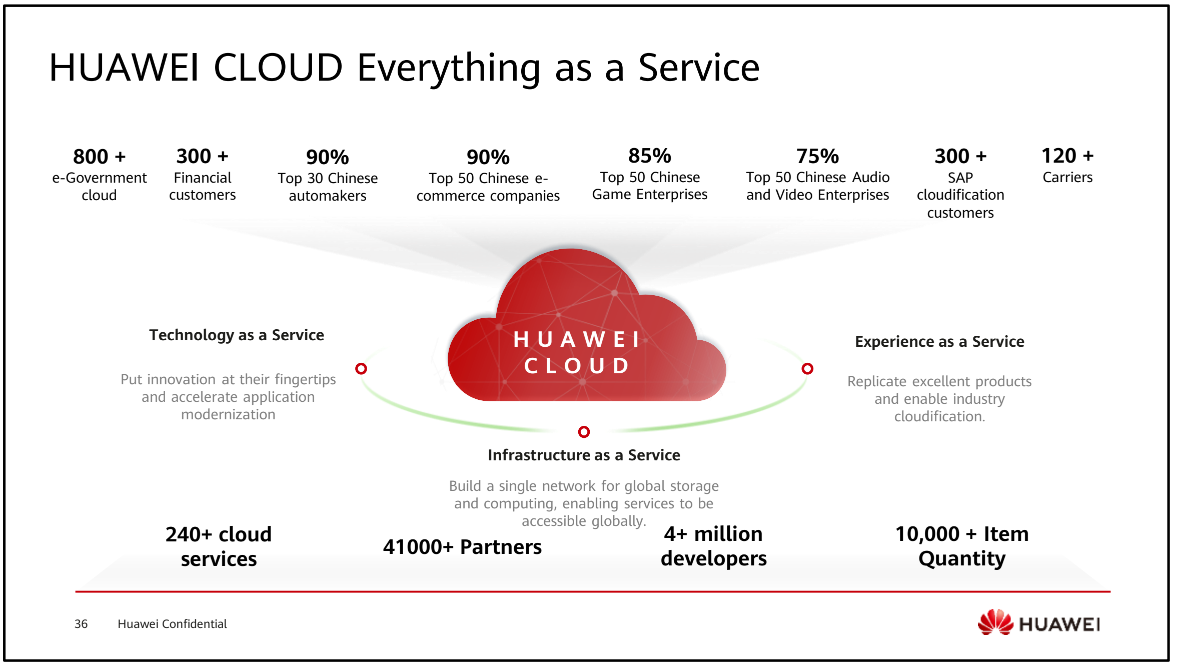
Private cloud: The cloud infrastructure is owned and managed for exclusive use by a single organization.
Public cloud: The cloud infrastructure is owned and managed by a third-party cloud service provider and shared with multiple organizations using the Internet.
Hybrid cloud: This is a combination of public and private clouds viewed from the outside as a single cloud.

Contents

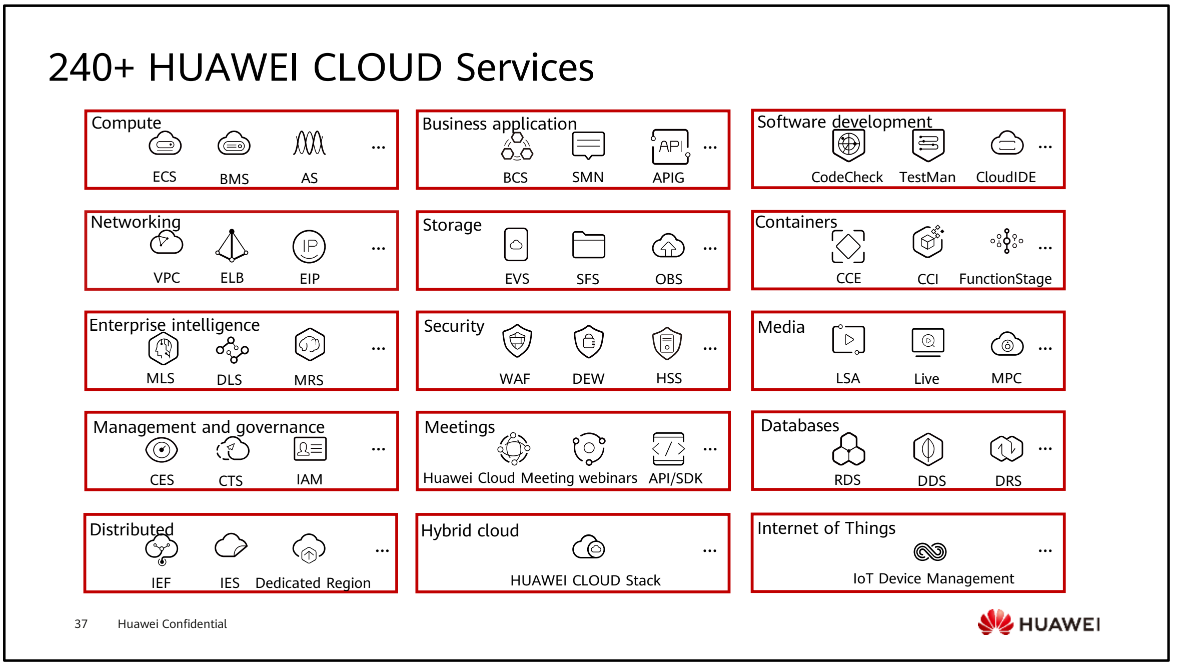
Vendors and representative technologies

HUAWEI	**HUAWEI CLOUD** is a one-stop cloud service platform launched by Huawei. It provides a wide range of cloud computing products and solutions. It aims to become a world-leading cloud computing service provider and help customers achieve digital transformation and business success. **Representing technologies** include Elastic Computing Service (ECS), Object Storage Service (OBS), Elastic Volume Service (EVS), Cloud Container Engine (CCE), etc.
Amazon	AWS, Amazon's cloud computing platform service. AWS provides users with a complete set of cloud computing services, including elastic computing, storage, databases, and applications, helping enterprises reduce IT investment and maintenance costs. **Representative technologies** include EC2, S3, RDS, etc.
Microsoft	Azure is Microsoft's cloud computing platform. It provides various cloud services, including computing, storage, database, and artificial intelligence. **Representative technologies** include virtual machines, Azure Blob storage, Azure SQL Database, etc.
Google	Google Cloud provides comprehensive cloud computing services, including computing, storage, database, and artificial intelligence. **Representative technologies** include Google Compute Engine, Google Cloud Storage, etc.
IBM	IBM Cloud provides a variety of cloud computing services, including computing, storage, databases, and artificial intelligence. **Representative technologies** include IBM Cloud Virtual Servers, IBM Cloud Object Storage, etc.
Alibaba	Alibaba Cloud is a cloud computing platform of Alibaba Group. It provides comprehensive cloud services, including computing, storage, database, and artificial intelligence. **Representative technologies** include Elastic Compute Service, Object Storage Service, etc.
VMware	VMware Cloud Foundation is a full-stack cloud infrastructure platform that provides a solution for quickly deploying and managing private, public, and edge clouds. **Representative technologies** include VMware vSphere, VMware NSX, VMware vSAN, VMware Workstation, etc.

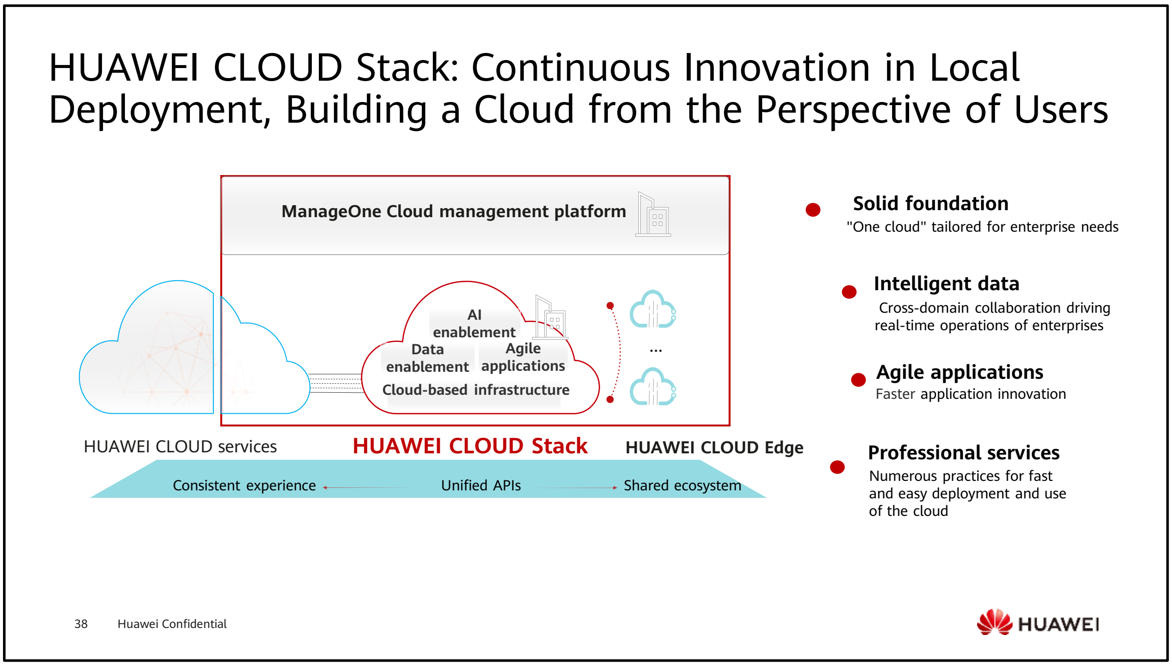
- VMware vSphere: VMware's core virtualization platform.
- VMware NSX：VMware‘s network virtualization and security platform.
- VMware vSAN：VMware's hyper-converged infrastructure (HCI) solution.
- VMware Workstation：desktop virtualization software for personal computers.



- In 2017, Huawei officially launched the HUAWEI CLOUD brand, which opens Huawei's 30-year-old technology accumulation and product solutions in the ICT field to customers. Through infrastructure as a service, technology as a service, and experience as a service, we realize "everything as a service". Provides stable, reliable, secure, reliable, and sustainable cloud services for customers, partners, and developers.
- Over the past few years, HUAWEI CLOUD adheres to technological innovation to lead industry development, strengthens software, and meets customers' diversified service requirements through system and architecture innovation. It has proposed leading technical concepts and best practices such as cloud native 2.0, distributed cloud, and application modernization. In addition, Huawei strives to become a trusted cloud. HUAWEI CLOUD is based on Huawei and understands enterprises better. It provides neutral, secure, and reliable cloud services, and works with partners to create win-win sharing and intelligent upgrades.
- Official website: https://www.huaweicloud.com/intl/en-us/



- HUAWEI CLOUD has continuously innovated and upgraded its full-stack cloud native technical capabilities. HUAWEI CLOUD has launched 240+ cloud services and 78,000+ APIs, aggregated more than 4,000+ global partners, developed more than 4 million developers, and released more than 10,000 applications in the cloud market.

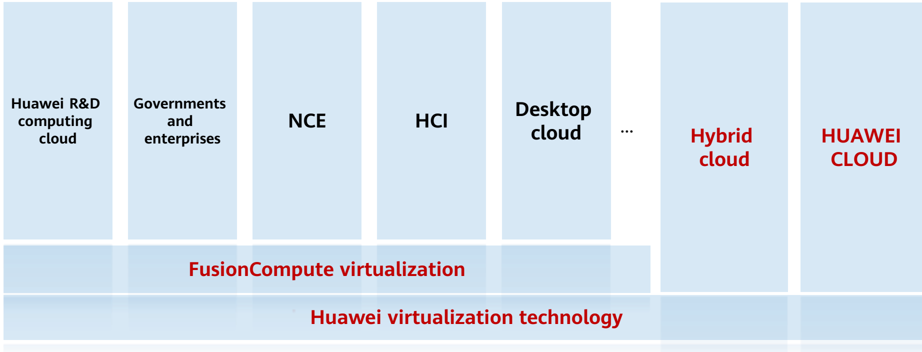


- HUAWEI CLOUD Stack is a full-stack cloud built by Huawei for governments and enterprises. It is derived from the full-stack service capabilities of Huawei public cloud. It meets users' compliance requirements through local deployment on the basis of unified APIs, unified experience, and unified ecosystem. It uses ManageOne to implement one cloud from the perspective of users and strives to become a cloud that understands government and enterprise better.
- HUAWEI CLOUD Stack and HUAWEI CLOUD are from the same door. HUAWEI CLOUD Stack has done a lot of standardization, lightweight, and engineering work, including automatic installation and deployment, upgrade, monitoring, and adaptation of southbound and northbound requirements. This puts forward high requirements on the technical background and agile development of vendors. HUAWEI CLOUD Stack will keep a proper pace to bring the most advanced services to customers.
- HUAWEI CLOUD Stack provides differentiated capabilities in the following four aspects:
  - **Solid foundation**: HUAWEI CLOUD Stack is the industry's only cloud with full-stack independent innovation capabilities. It implements end-to-end self-controllability from chips (Kunpeng + Ascend) to cloud platforms, operating systems (Euler OS), databases (GaussDB), and more. The ManageOne cloud management platform matches the government and

enterprise governance architecture, helping customers achieve one cloud from the perspective of users.

- **Intelligent data：** In the intelligent data field, HUAWEI CLOUD FusionInsight provides a big data cloud product portfolio that integrates the lake warehouse to accelerate data flow in the lake and provide customers with a sustainable big data platform.
- **Agile applications：** Through Huawei's IT digital transformation, Huawei incubates the ROMA solution to help customers smoothly evolve their applications and innovate cloud-native agilely.
- **Professional services：** Huawei continuously accumulates professional service capabilities, including blueprint top design, planning and construction, and O&M. Based on Huawei's global one-stop service layout and expert system, Huawei eliminates customers' concerns about cloudification and enables users to smoothly build, migrate, and use clouds throughout the lifecycle. To be the most trusted partner.

Huawei FusionCompute Virtualization Services Globally, Stable and Reliable



FusionCompute is the cornerstone of Huawei's global commercial solutions.

Build an internal R&D cloud to serve global R&D centers and provision more than 1 million VMs.

Served 12,000+ customers in 150+ countries and regions, and provisioned more than 5 million VMs.

- HCI: hyper-converged infrastructure.
- NCE: Network Cloud Engine.
- FusionCompute is Huawei's core virtualization product. It is a cloud operating system software that virtualizes hardware resources and centrally manages virtual resources, service resources, and user resources.
- FusionCompute is Huawei's earliest commercial cloud computing software. Its virtualization technology is proven and mature. In addition to the commercial solution FusionCompute, virtualization technologies also support cloud services of the entire company, including R&D computing cloud, hyper-convergence, and desktop cloud. Up to now, Huawei FusionCompute has been deployed for more than 12,000 customers in 150+ countries and regions, and has provisioned more than 5 million VMs.
- The following HCIA courses will introduce Huawei FusionCompute virtualization suite in detail.

Comparison Between FusionCompute, HUAWEI CLOUD Stack, and HUAWEI CLOUD

	FusionCompute	HUAWEI CLOUD Stack	HUAWEI CLOUD
Definition	A virtualization solution	A hybrid cloud solution	Cloud computing service platform
For Sales Targets	Enterprise	Enterprise	Enterprise or individual
Minimum Deployment Requirements	Physical servers, network devices, and storage devices	Physical servers, network devices, and storage devices	No hardware is required, and the Network Access
Initial investment	Hardware devices need to be purchased	Mode Subscription Service	No hardware is required, Pay-per-use
Scenario	Data center virtualization	Hybrid cloud, private cloud	Public cloud, hybrid cloud
Number of Services	VM and container	90+ cloud service	240+ cloud services

- FusionCompute virtualizes hardware resources. It uses virtual computing, storage, and network technologies to virtualize computing, storage, and network resources. FusionCompute is deployed on servers to virtualize hardware resources so that one physical server can function as multiple servers. In addition, unified interfaces are used to centrally schedule and manage these virtual resources, reducing service operating costs, ensuring system security and reliability, and helping carriers and enterprises build secure, green, and energy-saving cloud data centers.
- HUAWEI CLOUD Stack uses FusionSphere OpenStack as the cloud platform to integrate resources in physical data centers. ManageOne is used as the data center management software to manage multiple data centers in a unified manner. The cloud platform and data center management software work together to converge multiple data centers and improve the overall IT efficiency of enterprises. It also provides various cloud services, such as computing, storage, network, security, disaster recovery, and platform as a service (PaaS). In the following HCIP courses, we will introduce them in detail.

Quiz

1. Which of the following statements are true about challenges faced by traditional IT?
   A. Service rollout is slow.
   B. Expansion is difficult.
   C. It is not reliable enough.
   D. The TCO is too high.
2. Cloud computing deployment scenarios include public cloud, private cloud, and hybrid cloud.
   A. True
   B. False

Answers:

- ABCD
- A

Summary

- In this course, we have learned:
  - What IT is
  - IT development trend
  - Development of computing and virtualization technologies
  - What cloud computing is
  - The benefits of cloud computing
  - The service and deployment models for cloud computing
  - About technologies such as virtualization and resource pooling
  - What some of the main cloud computing vendors and technologies in the industry are
- In the subsequent courses, we will start with basic technologies to help you get a closer look at cloud computing.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Acronyms and Abbreviations

- APV: Advanced Power Virtualization
- IaaS: Infrastructure as a Service
- KVM: Kernel-based Virtual Machine
- LPAR: Logical Partition
- PaaS: Platform as a Service
- SaaS: Software as a Service

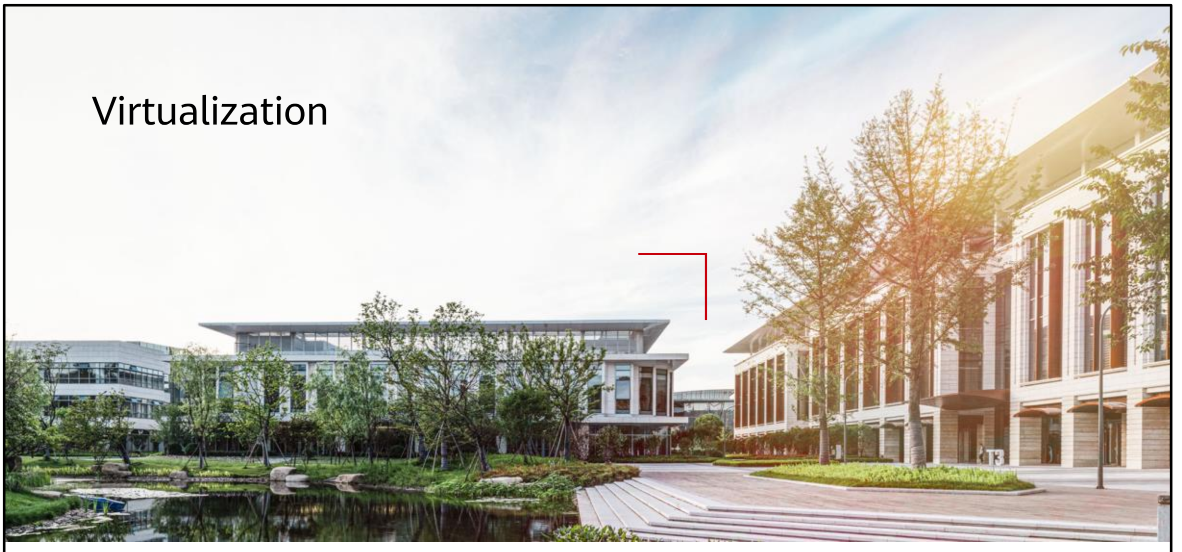
Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

Virtualization



Foreword

- Virtualization is the foundation of cloud computing, so what is virtualization? What is the essence of virtualization? What are mainstream virtualization technologies? This course will answer these questions and give you a brief introduction to virtualization.

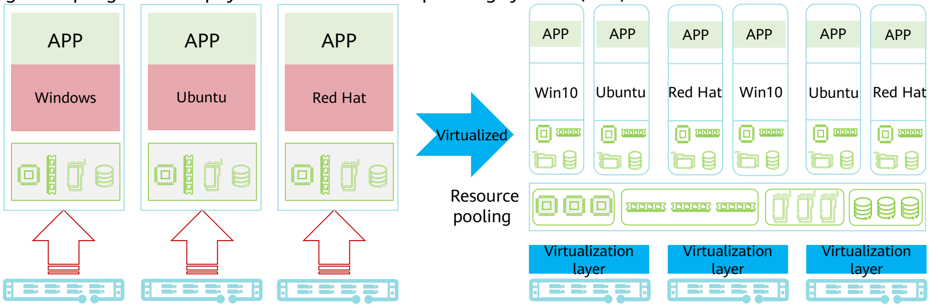
Objectives

- On completion of this course, you will be able to:
  - Describe the essence and value of virtualization.
  - Understand some of the mainstream virtualization technologies.
  - Grasp basic principles of mainstream virtualization technologies.

Contents

What Is Virtualization?

- Virtualization has a wide range of meanings. Any time you abstract resources from one form into another, that is virtualization, the creation of a logical representation of resources. Virtualization is an abstract layer that removes the tight coupling between physical hardware and operating systems (OSs).

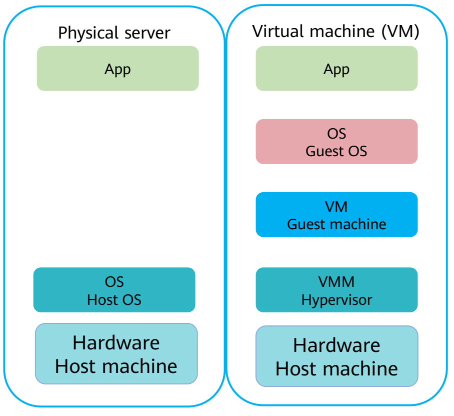


- IT resources are independent.
- OSs must be tightly coupled with hardware.

- Resources are virtualized to a shared resource pool.
- OSs are decoupled from hardware and resources are allocated to the OSs from the resource pool.

- Virtualization is the foundation of cloud computing. Simply speaking, virtualization allows multiple VMs to run on a physical server. The VMs share the CPU, memory, and input/output (I/O) hardware resources of the physical server, but are logically isolated from each other.
- In computer science, virtualization creates an abstraction layer over computer hardware for resource emulation, isolation, and sharing on one or multiple OSs.
- In essence, virtualization abstracts and simulates hardware resources. Virtualization abstracts a resource into one or more portions through space or time division and simulation.

Important Concepts of Virtualization



Guest OS

VM OS

Guest Machine

VM

Hypervisor

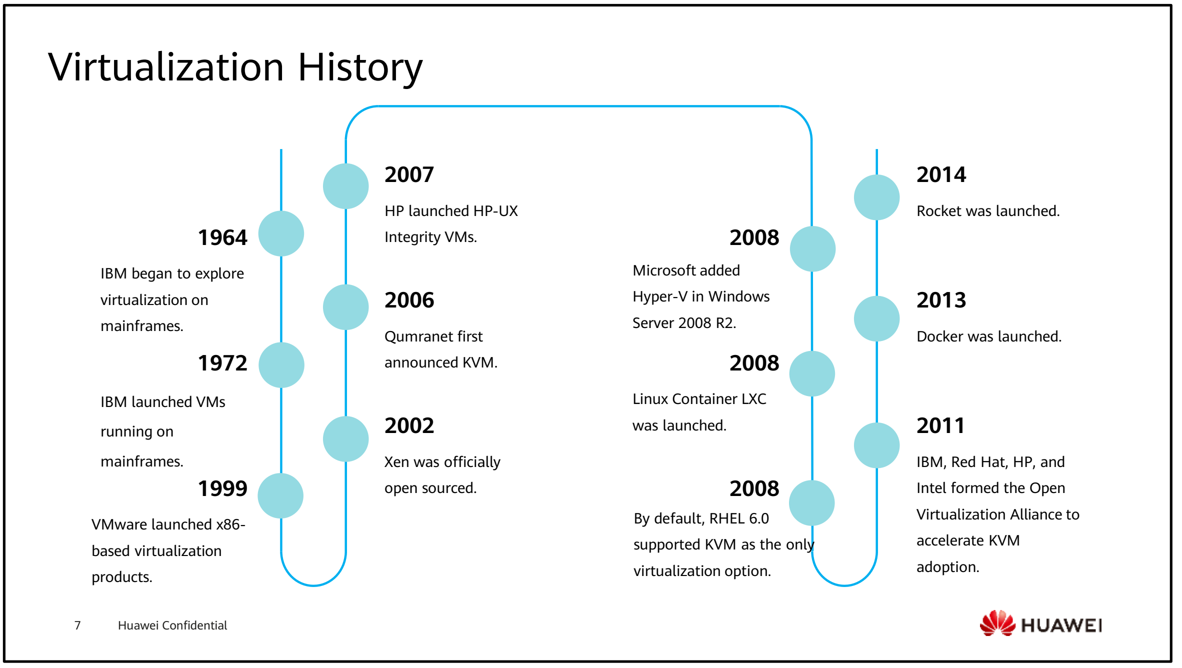
Virtualization software layer or virtual machine monitor (VMM)

Host OS

OS running on a physical machine (PM)

Host Machine

PM

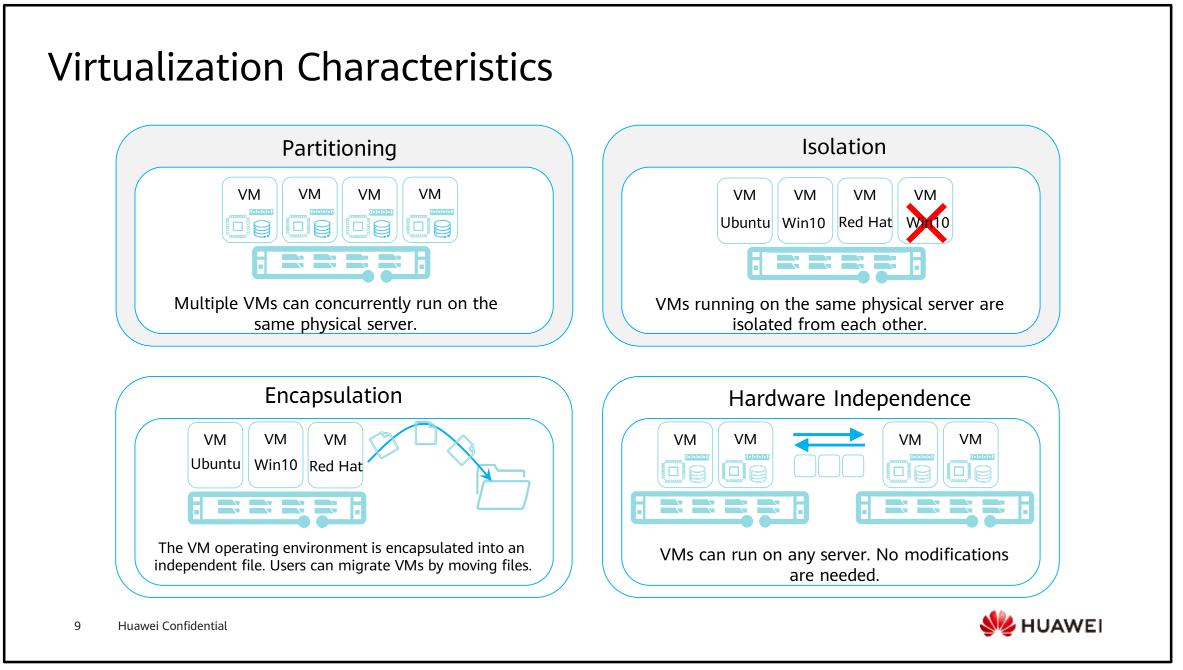


- In 1964, "Big Blue" IBM began experimenting with virtualization on mainframes.
- In 1972, IBM officially named System370's time-sharing system virtual machine.
- In 1999, VMware introduced the first virtualization product to run on the x86 architecture.
- In 2002, Xen was officially open source, and versions 1.0 and 2.0 were released. After that, Xen began to be integrated as a virtualization solution with Linux distributions such as Red Hat, Novell, and Sun. In 2004, Intel engineers began adding hardware virtualization support to Xen to prepare the necessary software for the upcoming new processors. Thanks to their efforts, Xen 3.0, released in 2005, officially supports Intel's VT technology and IA64 architecture. Therefore, Xen VMs can run operating systems without modification.
- In October 2006, Qumranet officially announced the birth of KVM after completing the optimization of basic functions, live migration, and major functions and performance. In October of the same year, the source code of the KVM module was officially incorporated into the Linux Kernel as a part of the kernel source code.
- Between 2006 and 2010, traditional IT vendors launched their own products in virtualization. In 2007, HP introduced Integrity virtual machines and Microsoft added Hyper-V to Windows Server 2008 R2. In November 2010, Red Hat introduced RHEL 6, a new enterprise edition of Linux, which integrates the latest KVM virtual machines and replaces Xen integrated in the RHEL 5.x series.
- In 2011, IBM, Red Hat, HP, and Intel established the Open Virtualization Alliance

to accelerate KVM promotion.

Virtualization Types

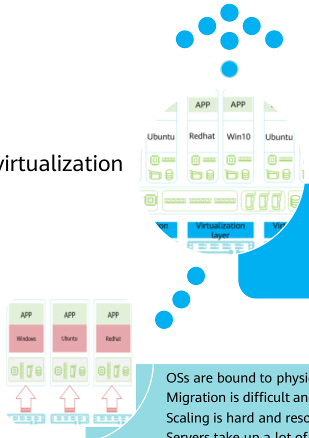
Type	Description
Full virtualization	The VMM virtualizes the CPU, memory, and device input/output (I/O) without modifying the guest OS and hardware. Full virtualization gives you excellent compatibility, but increases the load on the CPU of the host machine.
Paravirtualization	The VMM virtualizes CPU and memory and the guest OS virtualizes device I/O. The guest OS needs to be modified to coordinate with the VMM. Paravirtualization provides high performance but poor compatibility.
Hardware-assisted virtualization	Efficient full virtualization is realized with the help of hardware. Compatibility is good, and guest OSs do not need to be modified. This type of virtualization has been slowly eliminating differences between different software virtualization.



- Partitioning: The virtualization layer allocates server resources to multiple VMs whose OSs can be same with or different from each other. Each OS gains access only to its own virtual hardware, such as the virtual network interface card (NIC), virtual CPUs, and virtual memory, provided by the virtualization layer. Multiple apps run on the same physical server.
- Isolation: VMs that run on the same physical server are isolated from each other.
  - Even if one VM crashes or fails due to an OS failure, application crash, or driver failure, other VMs can still run properly.
  - If one VM is infected with worms or viruses, other VMs will not be affected as if each VM runs on an independent physical machine.
  - Resources can be managed to provide performance isolation. Specifically, you can specify the maximum and minimum resource usage for each VM to ensure that one VM does not use all resources.
  - Multiple loads, applications, or OSs can run concurrently on one PM, preventing problems that may occur on the x86 server, for example, application or dynamic link library (DLL) conflicts.
- Encapsulation: All VM data including the hardware configuration, BIOS configuration, memory status, disk status, and CPU status is stored into a group of files that are independent of physical hardware. This enables users to copy, save, and migrate VMs by copying, saving, and migrating files.
- Hardware independence: VMs run on the virtualization layer. Only virtual hardware provided by the virtualization layer can be accessed. The virtual hardware is independent of the physical server. In this way, the VM can run on any x86 server (IBM, Dell, HP, and more). No modifications are needed. This breaks the constraints between OSs and hardware and between applications and OSs/hardware.

Advantages of Virtualization

After virtualization



OSs are decoupled from physical servers.
Migration, scaling, and integration are all easy.
Standard virtual hardware consists of a series of files, so security is less work.

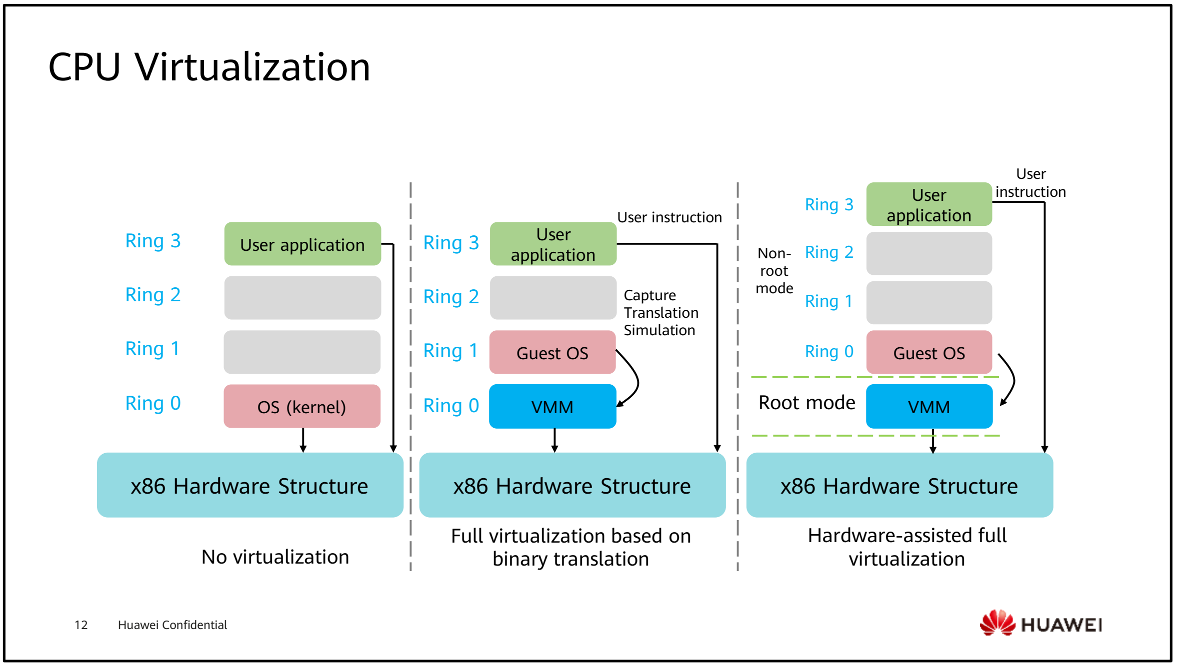
Before virtualization

OSs are bound to physical servers.
Migration is difficult and stability unreliable.
Scaling is hard and resource utilization low.
Servers take up a lot of space and need to be housed and maintained.

CPU Virtualization Issues

- CPU virtualization resolves the following two issues:
  - Simulation of CPU instructions (all sensitive instructions)
    - Sensitive instructions: Instructions that can read and write key system resources are called sensitive instructions.
    - Privileged instructions: The majority of sensitive instructions are privileged instructions, which can only be executed at the highest privilege level (kernel mode) of the processor.
  - Enabling multiple VMs to share CPUs
    - CPU virtualization uses a timer interruption mechanism similar to the time interruption mechanism used in native OSs. The timer interruption mechanism triggers the enabling of the VMM when an interruption occurs. The VMM then schedules resources in accordance with the preset scheduling policy.

- Key system resources: The interfaces presented by processors to software instruction sets and registers. The interfaces presented by I/O devices to software are status and control registers, collectively called system resources. Registers that affect the status and behavior of processors and devices are called key system resources.

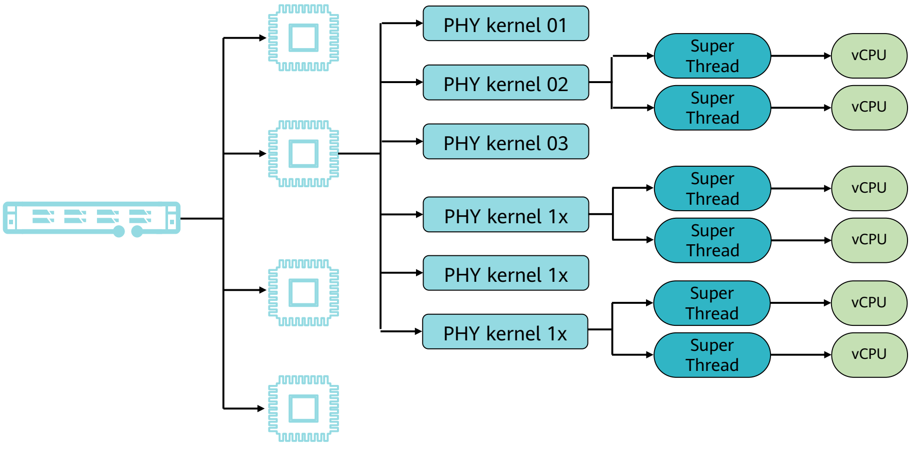


- FusionCompute uses hardware-assisted full virtualization.
- The x86 OS is designed to run directly on raw hardware devices and therefore is considered to fully occupy computer hardware. The x86 architecture provides four privilege levels for OSs and applications to access hardware. Ring indicates the CPU running level. Ring 0 is the highest level, Ring 1 is the second highest level.
  - A Linux or x86 OS (kernel) needs to directly access hardware and memory. The OS code needs to run on the highest level (Ring 0) so that the OS can use privileged instructions to control interruptions, modify page tables, and access devices.
  - The code of applications runs at the lowest running level (Ring 3), and controlled operations are not allowed. If you want to perform controlled operations (for example, access disks or write files), you need to execute system calls (functions). During system calls, the CPU running level is switched from Ring 3 to Ring 0, and the system calls the corresponding kernel code. This way, the kernel completes device access and then the CPU running level is switched back from Ring 0 to Ring 3. This process can also be described as switching between the user mode and kernel mode.
- However, this way of working gives rise to a problem. If the host OS is operating Ring 0, the guest OS cannot operate Ring 0. However, the guest OS cannot detect that the host OS is operating Ring 0. An error occurs if the guest OS does not have the permission to execute certain instructions it has previously executed. In this situation, the VMM is needed to resolve this problem. The VMM allows VM guest CPUs to access hardware based on the following three technologies:
  - Full virtualization
  - Paravirtualization

- Hardware-assisted virtualization

- Hardware-assisted virtualization technologies for processors include Intel's VT-x and AMD's AMD-V. New instructions and running modes allow the VMM to run in root mode and the guest OSs run in non-root mode at privilege level Ring 0. Generally, core instructions from the guest OS can reach the hardware and be executed without being transferred to the VMM. When the guest OSs receive special instructions, the system transfers the instructions to the VMM for processing.
- For example, the Intel VT technology introduces the VMX root operation mode and VMX non-root operation mode. Generally, the host OS and the VMM run in the VMX root mode, and the guest OS and its applications run in the VMX non-root mode. Both modes support all rings. Therefore, the guest machine can run in its desired rings (Ring 0 for the guest OS and Ring 3 for the applications), and the VMM runs in the ring required by the guest machine (for the KVM, QEMU runs in Ring 3 and KVM runs in Ring 0). The CPU switchover between the two modes is called VMX switchover. Switching from root mode to non-root mode is called VM entry. Switching from non-root mode to root mode is called VM exit. It can be seen that CPUs are controlled to switch between the two modes and execute the VMM code and guest OS code in turn.
- For a KVM VM, the VMM running in the VMX root mode executes VMLAUNCH instructions to switch the CPUs to the VMX non-root mode when the VMM needs to execute the guest OS instructions. The VMM then starts to execute guest OS code. This is the VM entry process. When the guest OS needs to exit the mode, the CPUs automatically switch to the VMX root mode. This is the VM exit process. If you look at the figure onscreen you can see that KVM guest OS code is controlled by the VMM and runs on physical CPUs. QEMU does not execute the code itself. It only controls VM code through KVM to allow the code to be executed by CPUs. The CPUs are not virtualized into virtual CPUs for the guest machines to use.

Mappings Between CPUs and vCPUs



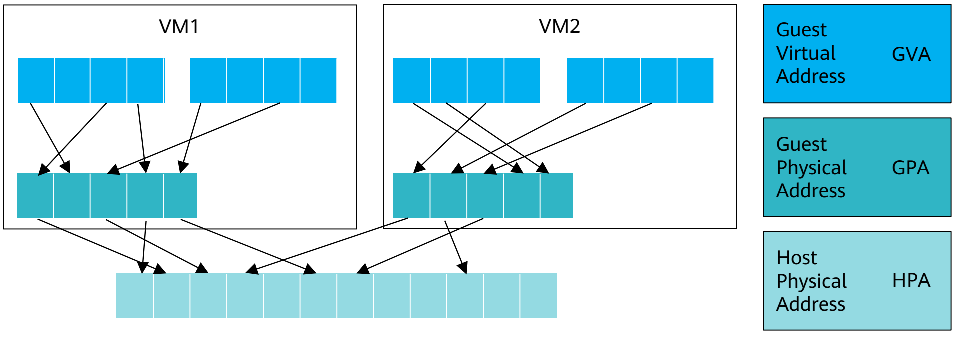
- This figure shows the mappings between vCPUs and CPUs.
- Let's take an RH server with the CPU frequency of 2.6 GHz as an example. A single server has two physical CPUs, each of which has eight cores. The hyper-threading technology provides two processing threads for each physical core. Each CPU has 16 threads, and the total number of vCPUs is 32 (2x8x2). The total CPU frequency is calculated as follows: 32 x 2.6 GHz = 83.2 GHz.
- The number of vCPUs on a VM cannot exceed the number of available vCPUs on a computing node agent (CNA) node. Multiple VMs can reuse the same CPU, and the total number of vCPUs running on a CNA node can exceed the actual number of vCPUs.

Memory Virtualization Issues

- Through memory management, a traditional native OS will ensure the following:
  - The memory starts from physical address 0.
  - Memory blocks have contiguous addresses.
- This approach to memory management gives rise to two issues:
  - Start from physical address 0: There is only one physical address 0, which cannot meet multiple concurrent customer requirements.
  - Contiguous addresses: Although consecutive physical addresses can be allocated, this method of memory allocation leads to poor efficiency and flexibility.
- Memory virtualization resolves both issues.

Memory Virtualization

- The physical memory of a PM is managed centrally, and is packed into multiple virtual memories for multiple VMs.
- KVM virtualizes and uses the physical memory and allocates it to VMs as required.



HUAWEI

- In KVM, the physical memory of a VM is the memory occupied by the qemu-kvm process. KVM uses CPU-assisted memory virtualization.
- Memory virtualization - shadow page table:
  - A memory management unit (MMU) on the host machine cannot directly load the page tables of guest machines for memory access. Address translations are required when a guest machine accesses the physical memory of host machines. That is, GVAs are translated to GPAs according to guest page tables, and then translated to host virtual addresses (HVAs) according to the mappings between GPAs and HVAs. Finally, HVAs are translated to HPAs according to host page tables. With shadow page tables, GVAs can be directly translated into HPAs.
  - Intel CPUs provide Extended Page Tables (EPT) to support the following translations on hardware: GVA -> GPA -> HPA, thereby simplifying and enhancing memory virtualization.
- To run multiple VMs on a machine, KVM needs to add a GPA, which is a not a real physical address. There is a translation layer: GVA -> GPA.
- However, the guest OS cannot directly access the actual machine memory. The VMM needs to map the guest physical memory to the host physical memory (GPA -> HPA).

I/O Virtualization Issues

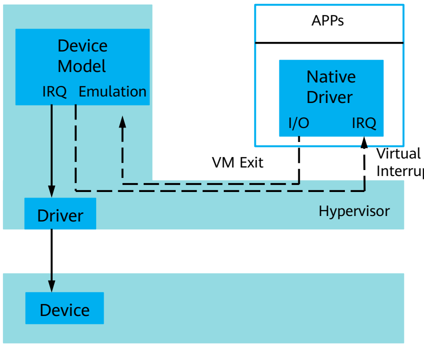
- FusionCompute I/O virtualization implements two functions:
  - Device discovery
    - FusionCompute controls which devices can be accessed by VMs.
  - Access interception
    - VMs access devices through I/O ports or MMIOs.
    - The device exchanges data with the memory through DMA.

I/O Virtualization

- I/O virtualization can be considered a hardware middleware layer between server components, OSs, and available I/O processing units. It allows multiple guest OSs to reuse limited peripheral resources.
- Device virtualization (I/O virtualization) is when you emulate the registers and memory of devices, intercept guest OS access to the I/O ports and registers, and use software to simulate device behavior.
- In Quick Emulator (QEMU)/KVM, guest machines can use emulators, Virtio devices, or PCI devices:
  - Emulators: devices that are completely emulated by the QEMU software
  - Virtio devices: paravirtualized devices that implement Virtio APIs
  - PCI devices: directly assigned

I/O Virtualization - Full Emulation

- Software is used to emulate a specific device.
  - The same software interface is used, for example: programmable input/output (PIO), memory mapped I/O (MMIO), direct memory access (DMA), or interrupt.
  - Virtual devices that are different from physical devices in the system can be emulated.
- Multiple context switches are required for each I/O operation.
  - VM <-> Hypervisor
  - QEMU <-> Hypervisor
- Devices emulated by software do not affect the software stacks of the VMs.
  - Native driver



- Advantages of I/O virtualization

Low dependency on the hardware platform

Convenient emulation of popular and legacy devices

High compatibility, requiring no additional support from host and guest machines

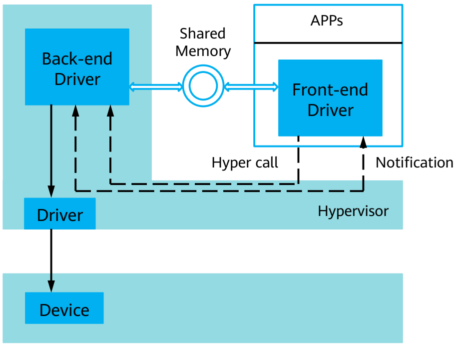
- Disadvantages of I/O virtualization

Poor performance due to long I/O path and large number of VM-Exists

I/O virtualization is applicable to scenarios that do not require high I/O or to emulating legacy devices (such as RTL8139 NICs).

I/O Virtualization - Virtio

- Virtualizing special devices
  - Special device drivers, including the front-end drivers on VMs and the back-end drivers on the hosts
  - Efficient communication between the front-end and back-end drivers
- Reducing the transmission overhead between VMs and hosts
  - Shared memory
  - Batched I/O
  - Asynchronous event notification mechanism (waiting/notification) between eventfd lightweight processes



- Advantages of Virtio paravirtualization

Implementing Virtio APIs

Reducing the number of VM-Exits

High execution efficiency of the guest machine I/O, better than common I/O emulation

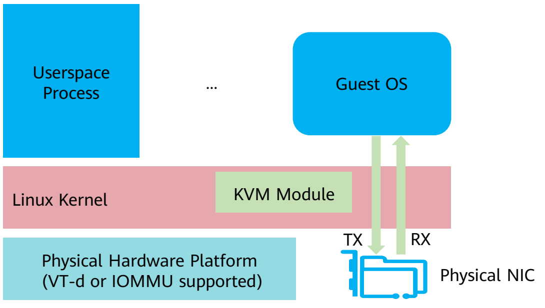
- Disadvantages of Virtio paravirtualization

Low compatibility due to lack of Virtio drivers in the guest machine (The earlier systems do not have the Virtio driver by default, and the Virtio driver must be additionally installed in the Windows.)

High CPU usage when I/O operations are frequent

PCI Device Assignment

- KVM VMs allow the PCI and PCI-E devices in the host machine to be attached to the guest VM so that the guest VM can exclusively access the PCI or PCI-E devices. After a device has been assigned to a guest VM by using the VT-d technology supported by the hardware, the guest VM treats the device as if it is physically connected to the VMs PCI or PCI-E bus, and the I/O interaction between the guest VM and the device is no different from interaction between two physical devices. The hypervisor rarely needs to participate in this process.

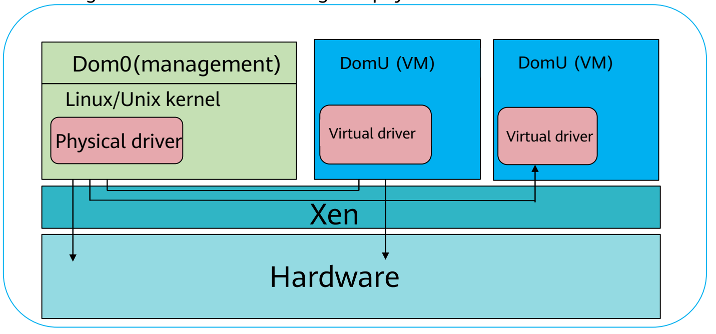


- PCI device assignment enables guest machines to fully occupy PCI devices. In this way, when I/O operations are performed, the number of VM-Exits is greatly reduced, so that the VM-Exits do not get trapped in the hypervisor. This greatly improves the I/O performance and in fact achieves almost the same performance as a non-virtualized system. Although the performance of Virtio is good, VT-d overcomes the problems of poor compatibility and high CPU usage. However, VT-d has its own disadvantages. Space on a server mainboard is limited, and the number of PCI and PCI-E devices that can be added is limited. If a host machine has a large number of guest machines, it is difficult to allocate VT-d devices to each guest machine independently. In addition, a large number of VT-d devices are independently assigned to guest machines, increasing the number of hardware devices and hardware investment costs.

Contents

Xen Virtualization

- The Xen hypervisor is the first program that is loaded after a server is enabled through BIOS. Then, a VM, with specific permissions, is enabled, which is called Domain 0 (Dom0). The operating system of Dom0 can be Linux or Unix. Dom0 controls and manages the Hypervisor. Of all the VMs, Dom0 is the only one that can directly access physical hardware such as a storage device and a network interface card (NIC). It serves as a bridge for Domain U (DomU) to access storage devices and NICs through its physical drive.



23 Huawei Confidential HUAWEI

- Xen was initially an open-source research project of Xensource founded by Cambridge University. In September 2003, Xen 1.0 was released. In 2007, Xensource was acquired by Citrix, and then Xen was promoted by Xen Project (www.xen.org), whose members include individuals and companies (such as Citrix and Oracle). In March 2011, the organization released Xen 4.1.
- Xen not only supports the x86/x86_64 CPU architecture of CISC that both ESX and Hyper-V support but also RISC CPU architectures (IA64 and ARM).
- Xen supports two types of virtualization: Paravirtualization (PV) or hardware virtual machine (HVM). PV requires OSs with specific kernels, for example, the Linux kernel based on the Linux paravirt_ops (a set of compilation options of the Linux kernel) framework. However, Xen PV does not support Windows OSs due to its closeness. There is something special for Xen PV: CPUs are not required to support hardware-assisted virtualization, which is applicable to the virtualization of old servers produced before 2007. Xen HVM supports native OSs, especially Windows OSs, and Xen HVM requires CPUs to support hardware-assisted virtualization. It can modify all hardware (including the BIOS, IDE controllers, VGA video cards, USB controllers, and NICs) emulated by QEMU. To improve I/O performance, paravirtualized devices replace emulated devices for disks and NICs in full virtualization. Drivers of these devices are called PV on HVM. To maximize performance of PV on HVM, the CPU must support MMU hardware-assisted virtualization.
- The Xen hypervisor layer has less than 150,000 lines of code. In addition, it, similar to Hyper-V, does not include any physical device drivers. The physical device driver loaded in Dom0 can reuse the existing drivers in Linux. Xen is

compatible with all hardware Linux supports.

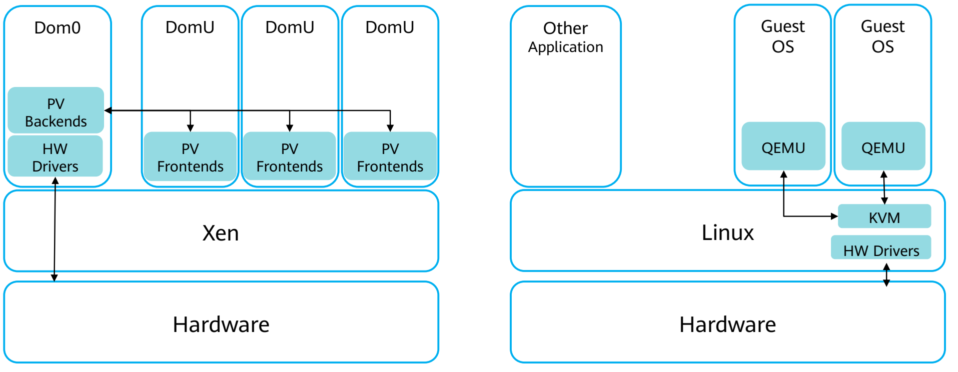
KVM Virtualization

- KVM is a kernel-based VM.
- The essence of KVM is kvm.ko, a virtualization module in the Linux kernel. It uses Linux to perform operations, such as task scheduling, memory management, and interaction with hardware devices.
- KVM is open-source software that was integrated into the Linux 2.6.20 kernel in February 2007.
- In KVM, a VM is a Linux process scheduled by the CPU.
- A KVM runs in the kernel space and provides CPU and memory virtualization. It does not perform any simulation. QEMU runs in user space, where it provides virtualization emulation of hardware I/O.

- KVM is short for Kernel-based Virtual Machine. It was originally an open source project developed by Qumranet, which was acquired by Red Hat in 2008. However, KVM is still an open-source project supported by venders such as Red Hat and IBM.
- KVM is a kernel-based VM because KVM is a Linux kernel module. After this module is installed on a physical machine running Linux, the physical machine becomes a hypervisor without affecting other applications running on Linux.
- KVM supports CPU architectures and products, such as x86/x86_64 CPU architecture (also for Xen), mainframes, midrange computers and ARM architecture.
- KVM makes full use of the hardware-assisted virtualization of CPU and reuses many functions of the Linux kernel. As a result, KVM consumes a few resources. Avi Kivity, the founder of KVM, claimed that the KVM module had only about 10,000 lines of code. However, we cannot naturally conclude that KVM hypervisor just had the amount of code, because KVM is actually a module that can be loaded in the Linux kernel. It is used to turn the Linux kernel into a hypervisor.
- A Linux kernel is converted into a hypervisor by loading a KVM module. The Linux runs in kernel mode, a host process runs in user mode, and a VM runs in guest mode, so the converted Linux kernel can perform unified management and scheduling on the host process and the VM. This is why KVM got its name.
- KVM history:
  - In October 2006, Qumranet, an Israeli company, released KVM.
  - In December 2006, KVM was integrated into the kernel (Linux 2.6.20rc).
  - In February 2007, Linux 2.6.20 was officially released.
  - In September 2008, Red Hat acquired Qumranet for $107 USD million.
  - In September 2009, RHEL 5.4 started to support KVM and Xen.

- Since November 2010, RHEL 6.0 and later versions have been supporting KVM only.

Xen vs. KVM

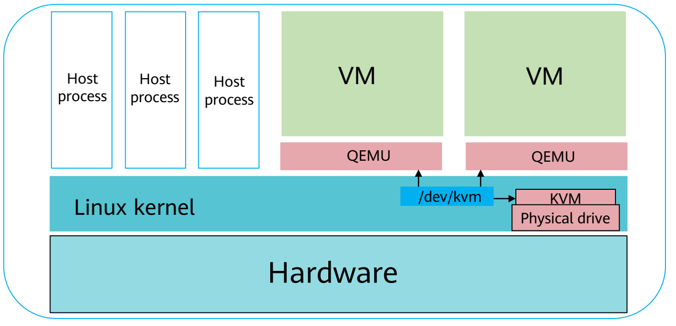


HUAWEI

- The Xen platform architecture focuses on security. To ensure security, the access of domains to the shared zone must be authorized by the hypervisor.
- The KVM architecture focuses on performance. The access and mapping of the shared zone between VMs or between VMs and the host kernel do not need to be authorized by the hypervisor, so the access path is short.

KVM and QEMU

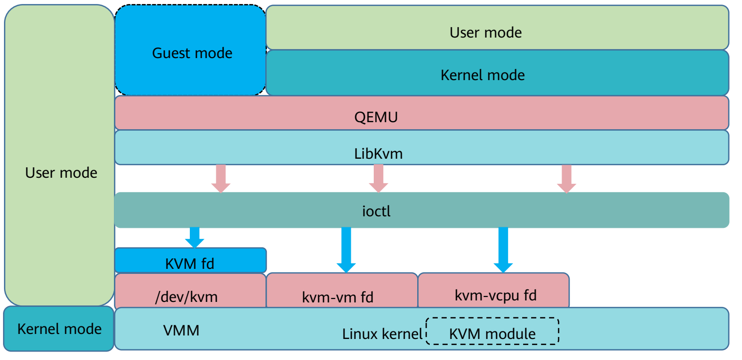
- In the KVM virtualization solution, KVM virtualizes CPU and memory, and QEMU virtualizes I/O devices.
- QEMU is software-based open-source (emulation) software. It can fully emulate all resources required by VMs, including the CPU, memory, I/O device, USB, and NIC.



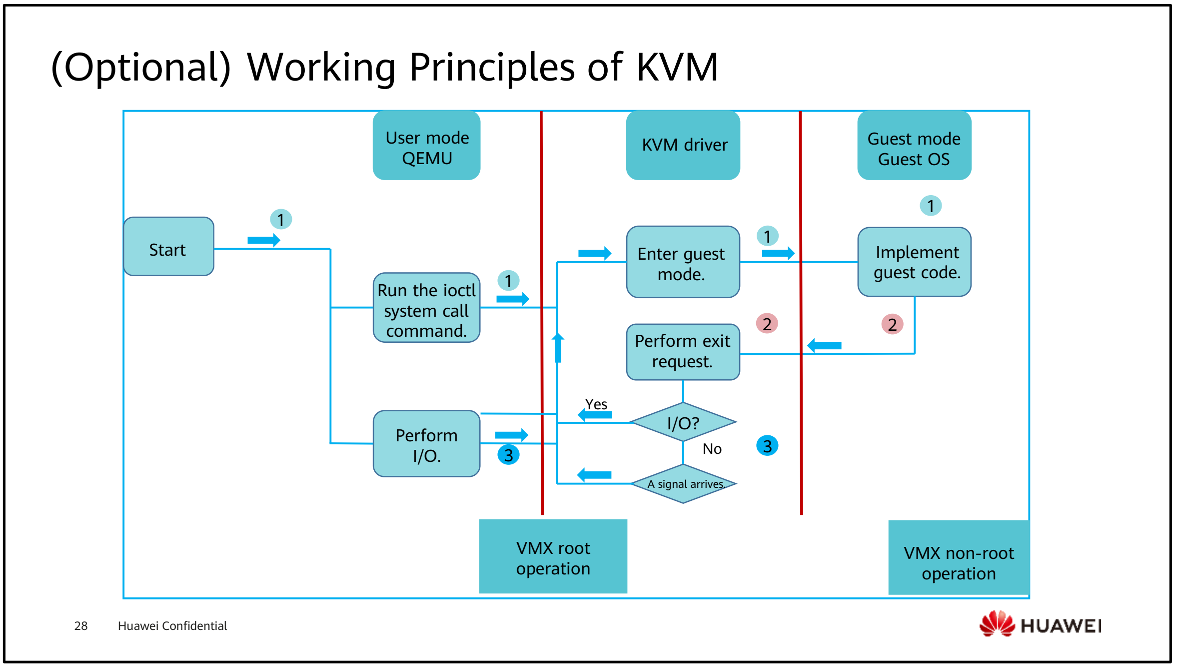
- KVM is used to emulate CPU running, but does not support networks and I/O. QEMU-KVM is a complete KVM-based emulator and supports complete I/O simulation. To achieve cross-VM performance, OpenStack does not directly control QEMU-KVM but uses the Libvirt library to control QEMU-KVM. We will introduce Libvirt later.
- KVM cannot be separated from QEMU. To simplify development and reuse code, KVM was modified based on QEMU at the early stage. CPU virtualization and memory virtualization that consume much CPU performance are transferred and implemented in the kernel, while the I/O virtualization module is reserved for implementation in the user space. This avoids frequent switching between the user mode and kernel mode and optimizes performance.
- QEMU cannot be separated from KVM either. QEMU is emulated by pure software and runs on user controls, so it has poor performance. QEMU uses KVM virtualization to accelerate its VMs and provide resources for them.
- The /dev/kvm interface bridges QEMU and KVM. /dev/kvm is a device file. You can use the ioctl function to control and manage this file to implement data interaction between user space and kernel space. The communication process between KVM and QEMU is a series of ioctl system calls for /dev/kvm.

Working Principles of KVM

- KVM is a module of the Linux kernel and it runs in kernel space.
- QEMU running in user space is used to virtualize I/O devices.
- After the KVM module is installed in Linux, there are three modes: guest mode, user mode, and kernel mode.



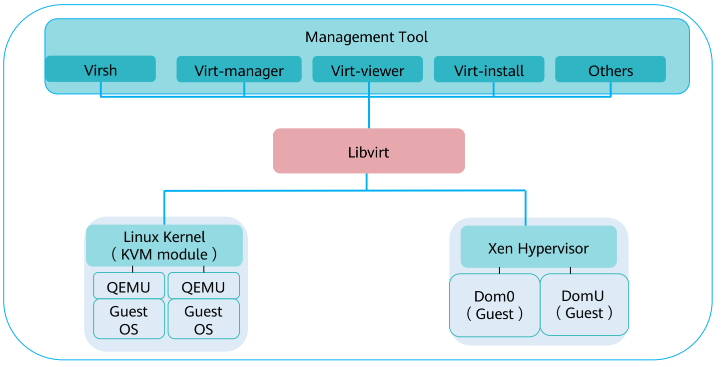
- This figure shows the basic structure of KVM. KVM is a kernel module and is regarded as a standard Linux character set device (/dev/kvm). QEMU uses the file descriptor (fd) and ioctl to send VM creation and running commands to the device driver through the Libkvm API. KVM can parse commands.
- The KVM module enables the Linux host to function as a VMM. The guest mode is added except for the modes originally existed. There are three working modes for VMs:
  - Guest mode: executes non-I/O guest code. VMs run in this mode.
  - User mode: executes I/O instructions on behalf of a user. QEMU runs in this mode to simulate I/O operation requests for VMs.
  - Kernel mode: It can switch to the guest mode and process VM-Exit caused by I/O or other instructions. The KVM module works in the kernel mode where hardware can be operated. To this end, the guest OS needs to submit a request to the user mode when performing an I/O operation or a privileged instruction, and then the user mode initiates a hardware operation to the kernel mode.



- QEMU in user mode uses Libkvm to enter kernel mode through ioctl. After creating virtual memory and virtual CPUs for the VM, the KVM module executes the VMLAUCH instruction to enter the guest mode and loads the guest OS.
- If an external interruption occurs on the guest OS or the shadow page table is missing, the guest OS exits the guest mode and enters the kernel mode for exception handling. Then, the guest OS enters the guest mode again and executes the guest code.
- If an I/O event occurs or a signal in the signal queue arrives, the signal instruction goes into user mode (QEMU) for further processing and emulation is performed.

Virtualization Platform Management Tool - Libvirt

- Libvirt is a set of APIs developed using C. It aims to provide a universal and stable software layer to manage multiple virtualization methods on PMs and VMs, and it also supports remote management.
- Libvirt is a virtualization library in Linux and also an open-source project. It is a powerful virtualization platform management tool. The managed virtualization platform can be KVM, Xen, VMware, or Hyper-V.



- In different virtualization scenarios, many solutions (such as KVM and Xen) are proposed. To support more vendors and service areas, many IaaS solutions need to integrate lots of virtualization. To this end, Libvirt provides a platform management tool for users, supporting multiple virtualization solutions.
- Libvirt, an open-source API, daemon, and management tool, is designed to manage virtual guest machines, virtual networks, and storage.
- Through a driver-based architecture, Libvirt supports different hypervisors. Loaded drivers vary for hypervisors: Xen driver for Xen and QEMU driver for QEMU or KVM.
- Libvirt works as an intermediate adaptation layer. It shields details of hypervisors, so the hypervisors are completely transparent to the management tool of the user space. By doing so, Libvirt provides a unified and stable API for the management tool.

Quiz

1. In full virtualization, VMM is used for CPU and memory virtualization, and the Guest OS is used for device I/O virtualization. The guest OS needs to be modified to coordinate with the VMM. This method provides high performance but poor compatibility.
   A. True
   B. False
2. Libvirt is a virtualization library on Linux. It aims to provide a universal and stable software layer to manage multiple virtualization modes and VMs on PMs and supports remote management.
   A. True
   B. False

- Answers
  - B
  - A

Summary

- In this course, we have learned the essence and value of virtualization, mainstream virtualization technologies, and basic principles of mainstream virtualization technologies. In the following course, we will continue to learn the features of Huawei virtualization platform.

Recommendations

- Huawei Learning
  - http://e.huawei.com/en/talent/portal/#/
- Huawei Support Case Library
  - http://support.huawei.com/enterprise/en/knowledge?lang=en

Acronyms and Abbreviations

- KVM: Kernel-based Virtual Machine
- VMM: Virtual Machine Monitor

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

Huawei Virtualization Platform

Foreword

- This chapter describes the basic concepts, architecture, and positioning of Huawei FusionCompute virtualization platform, and the functions, planning, and deployment of FusionCompute virtualization products.

Objectives

- On completion of this course, you will be able to:
  - Describe the basic components of the FusionCompute virtualization suite.
  - Understand the architecture, positioning, and features of FusionCompute.
  - Familiarize yourself with the functions of FusionCompute.
  - Understand the FusionCompute planning and deployment.

Contents

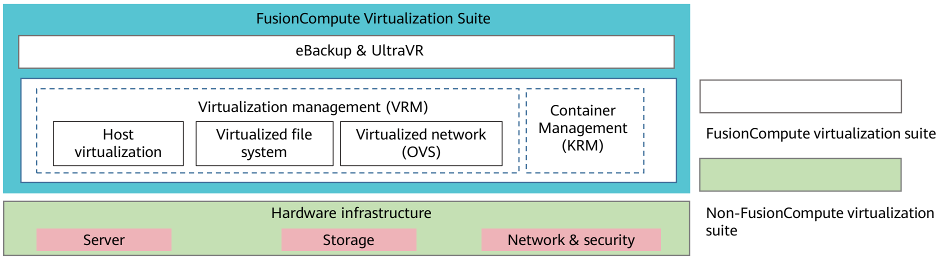
HUAWEI

FusionCompute Virtualization Suite (1)

- Huawei FusionCompute virtualization suite is an industry-leading virtualization solution. This solution significantly improves data center infrastructure efficiency and provides the following benefits for customers:
  - Improve infrastructure resource utilization in data centers.
  - Significantly accelerate service rollout.
  - Substantially reduce power consumption in data centers.
  - Leverage high availability (HA) and powerful restoration capabilities of virtualized infrastructure to provide rapid fault recovery for services, thereby cutting data center costs and increasing system runtime.

FusionCompute Virtualization Suite (2)

- The FusionCompute virtualization suite virtualizes hardware resources using the virtualization software deployed on physical servers, so that one physical server can function as multiple virtual servers. This solution maximizes resource utilization by centralizing existing VMs workloads on some servers and therefore releasing more servers to carry new applications and solutions.



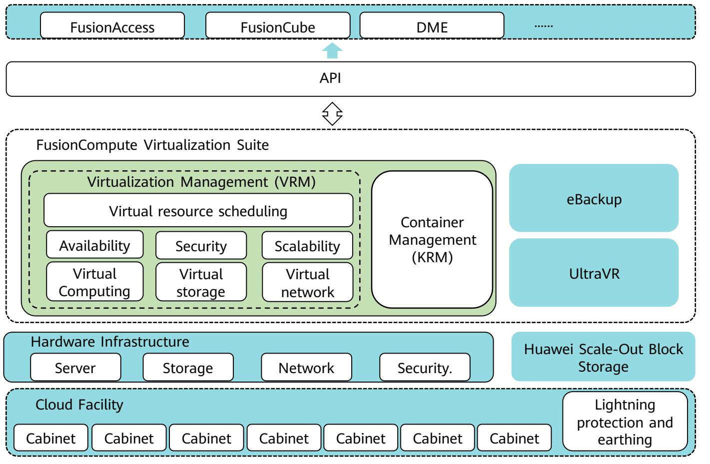
- Application Scenario:
  - Single-hypervisor applies to scenarios in which an enterprise only uses FusionCompute as a unified operation, maintenance, and management platform to operate and maintain the entire system, including monitoring resources, managing resources, and managing the system. FusionCompute virtualizes hardware resources and centrally manages virtual resources, service resources, and user resources. It virtualizes compute, storage, and network resources using the virtual computing, virtual storage, and virtual network technologies. FusionCompute centrally schedules and manages virtual resources using a unified interface, thereby reducing the operating expense (OPEX) and ensuring high system security and reliability.
- FusionCompute is mandatory, eBackup and UltraVR are optional.

Contents

HUAWEI

FusionCompute Positioning

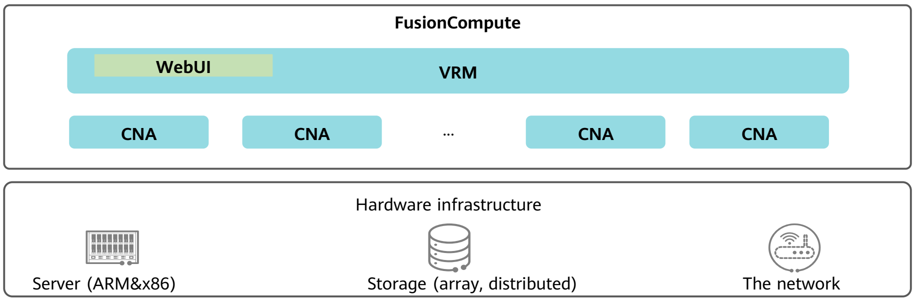
- FusionCompute is a cloud OS. It virtualizes hardware resources and centrally manages virtual resources, service resources, and user resources. It virtualizes compute, storage, and network resources using the virtual computing, virtual storage, and virtual network technologies.
- FusionCompute provides high system security and reliability, and reduces the OPEX, helping carriers and enterprises build secure, green, and energy-saving data centers.



- In addition to the commercial solution FusionCompute, virtualization technologies also support Huawei's services, such as hyper-converged FusionCube, and desktop cloud FusionAccess.
- The FusionCompute container management feature provides an enterprise-level K8s platform and supports tenant project management, cluster lifecycle management, container image and application management, and container monitoring and O&M. It is an optimal foundation platform for application modernization.
- Cloud facilities refer to the auxiliaries and space required by the cloud data center, including the power supply system, fire-fighting system, wiring system, and cooling system.
- Hardware infrastructure consists of servers, storage devices, network devices, and security devices. These resources allow customers to build different scale systems and expand its capacity based on actual needs, and to use applications ranging from the entry level to the enterprise level. Various devices provide customers with multiple and flexible choices.
- Huawei Distributed Block Storage is a scale-out storage software product that integrates storage and compute capabilities. It can be deployed on general-purpose servers to consolidate the local disks on all the servers into a virtual storage resource pool, aiming to provide the block storage function.
- eBackup is a virtualized backup software product, which works with the FusionCompute snapshot function and the Changed Block Tracking (CBT) function to back up VM data.
- UltraVR is a DR management software product, which provides data protection and DR for the key VM data using the asynchronous remote replication feature provided by the underlying SAN storage system.

FusionCompute Architecture

- FusionCompute consists of the following modules:
  - Compute Node Agent (CNA) deployed on the server that needs to be virtualized.
  - Virtual Resource Management (VRM) is deployed on VMs or physical servers. VRM provides web pages for management and maintenance personnel.



- CNA is short for Compute Node Agent. CNAs can be deployed on servers that need to be virtualized.
- VRM is short for Virtual Resource Management. VRM nodes can be deployed on VMs or physical servers. VRM provides a web interface for management and maintenance personnel.

FusionCompute Modules

Module	Description	Function
CNA	Compute Node Agent (CNA), deployed on the server to be virtualized.	• Implementing the virtual computing function. • Managing the VMs running on compute nodes. • Managing compute, storage, and network resources on compute nodes.
VRM	Virtual Resource Management (VRM) can be deployed as a VM or on a physical server. VRM provides web pages for management and maintenance personnel.	• Managing block storage resources in a cluster. • Managing network resources, such as IP addresses and virtual local area network (VLAN) IDs, in a cluster and allocating IP addresses to VMs. • Managing the lifecycle of VMs in a cluster, and distributing and migrating VMs across compute nodes. • Dynamically adjusting resources in a cluster. • Implementing centralized management of virtual resources and user data, and providing elastic computing, storage, and IP address services. • Allowing O&M engineers to remotely access FusionCompute through one unified web interface to perform resource monitoring and management and view resource statistics reports.

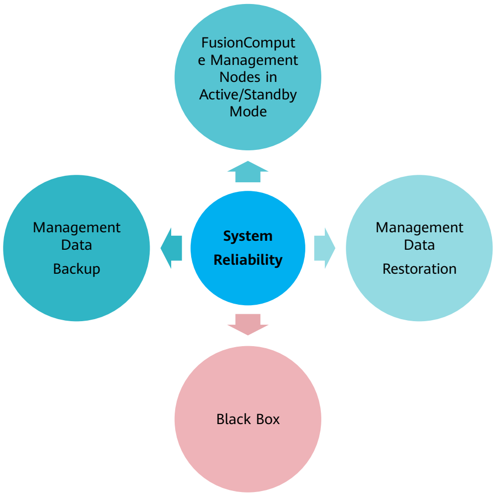
Contents

Main Functions and Features of FusionCompute

Computing Virtualization	Storage Virtualization	Network Virtualization
Cluster and Host Resource Management VM Resource Management VM Lifecycle Management VM Template Management Computing Performance Enhancement (NUMA) Distributed resource scheduling (DRS/DPM/affinity) VM Snapshot VM Peripherals GPU Passthrough	Storage Resource Management Virtual Volume Lifecycle Management Virtual File System (VIMS) Storage QoS Thin provisioning Online Virtual Volume Expansion Virtual Volume Migration Raw Device Mapping (RDM)	Network Resource Management Distributed Virtual Switch Port Group Network QoS SR-IOV User-mode OVS IPv6

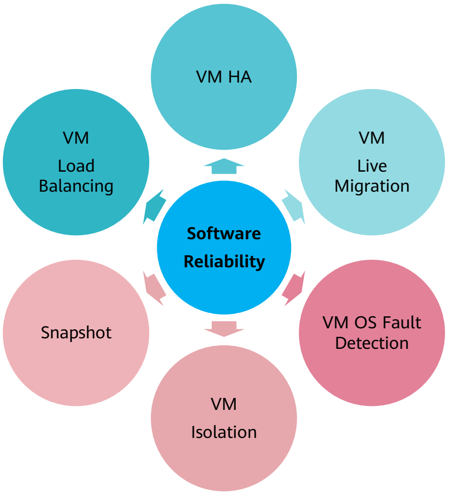
O&M Management	High Availability	Disaster Recovery and Backup
Permission management (user/role) Alarm Monitoring System Configuration Topology display Upgrade/Patching Information Collection Tool Health Check Tool	Management Reliability (Active/Standby, Black Box, and Backup) VM HA **Security** Virtualization Antivirus Management Security Data Security Protocol Security	VM Backup Intra-city high availability of VMs VM Active/Standby DR Metropolitan Active-Active DR

FusionCompute System Reliability

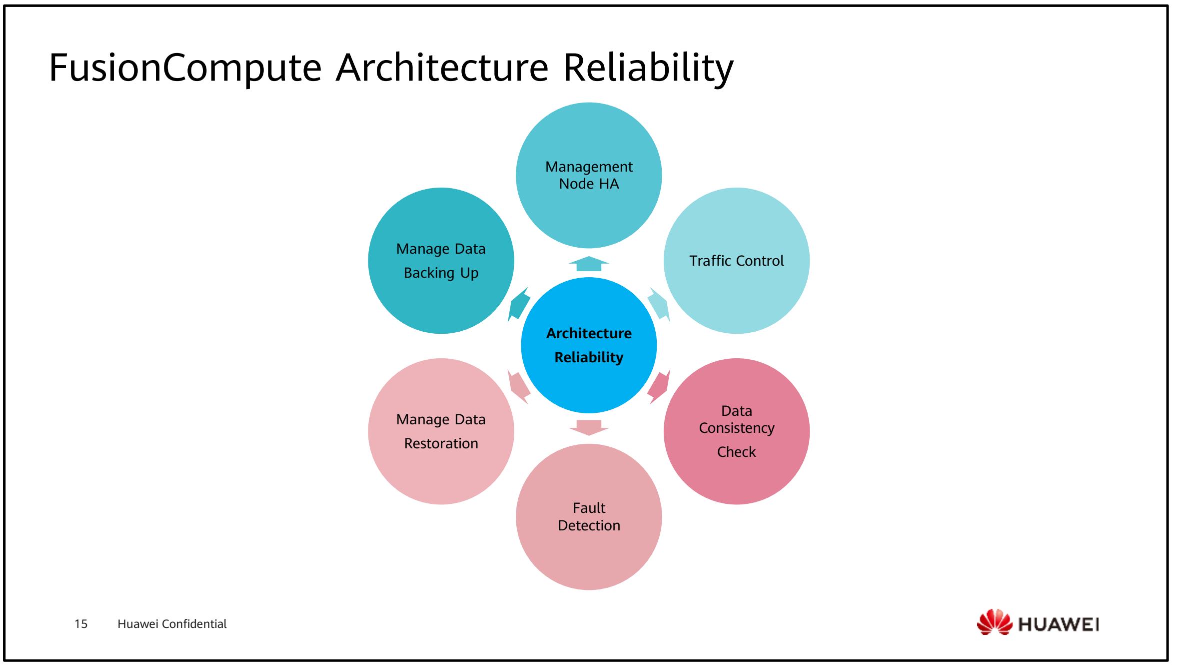


- FusionCompute Management Nodes in Active/Standby Mode:
  - FusionCompute management nodes are deployed in active/standby mode. If any fault occurs, such as a hardware failure, suspended key process, OS panic, or network interruption, the standby node automatically takes over for the active node in 1 or 2 minutes, continuing to provide virtualization management services.
- Host OS Fault Locating Tool of FusionCompute: Black Box:
  - Each FusionCompute host OS has a black box embedded. This black box stores fault information about the virtualization OS kernel, facilitating kernel fault locating and restoration.
- Management Data Backup and Restoration:
  - The system periodically backs up the configuration data and service data on local and remote devices. If any management node service fails and cannot be automatically restored, it can be restored using the local data backup rapidly. If a catastrophic failure occurs, both the active and standby management nodes are faulty and cannot be restored by restarting, FusionSphere allows users to restore these nodes using the remote data backup, thereby shortening the service restoration duration.

FusionCompute Software Reliability



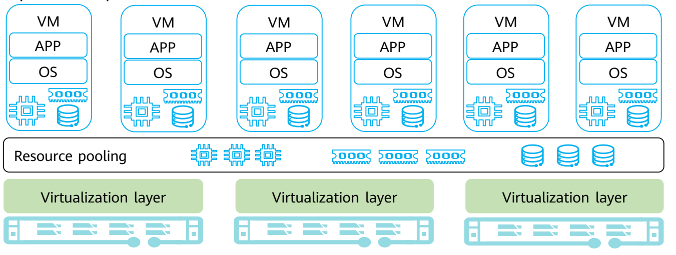
- VM HA: The VM HA feature ensures quick recovery of a VM. With this feature, when a VM is faulty, the system automatically re-creates the VM on another normal compute node.
- VM Live Migration: If users migrate the VMs from one server to another server without interrupting the service, it is called live migration of VMs. The VM manager provides quick recovery of memory data and memory sharing technologies to ensure that the VM data before and after the live migration remains unchanged.
- VM Load Balancing: In the load balancing mode, the system dynamically allocates the load based on the current load status of each physical server node to implement load balancing in a cluster.
- Snapshot: The snapshot feature enables FusionCompute to restore a damaged VM using its snapshots.A snapshot stores VM status information (including hard disk information) at a certain point of time..
- VM Isolation: FusionCompute supports information isolation between VMs. When multiple VMs are running on the same physical server, the VMs are independent of each other. The fault of one VM does not affect the running of other VMs.
- VM OS Fault Detection: If a VM becomes faulty due to a VM failure or physical server failure, the system automatically restarts the faulty VM from the physical server where the VM is located or from another physical server, depending on the preset policy.
- Black box: The black box embedded in FusionCompute collects information about the system. If a fault occurs, the black box collects and stores the last information about the system. This facilitates fault locating.



- Management Node HA: Management nodes work in active/standby mode to ensure HA. If the active node is faulty, the standby node takes over services from the active node, ensuring uninterrupted service processing of management nodes.
- Management Data Backup and Restoration: The system periodically backs up the configuration data and service data on local and remote devices. If the management node service becomes abnormal and cannot be automatically restored, it can be restored using the local data backup rapidly. If a devastating fault occurs, both the active and standby management nodes are faulty at the same time, and they cannot be restored by restarting, they can be restored using the remote data backup rapidly (within 1 hour). With this service, the time for restoration is reduced.
- Traffic Control: The traffic control mechanism helps the management node provide concurrent services of high availability without system collapse due to excessive traffic. Traffic control is enabled for the access point, so that excessive load on the front end can be prevented to enhance system stability.
- Fault Detection: The system provides the fault detection and alarm reporting functions, and the tool for displaying fault on web browsers.
- Data Consistency Check: The FusionCompute periodically performs data consistency checks to ensure data consistency.

FusionCompute Product Functions - Virtual Computing

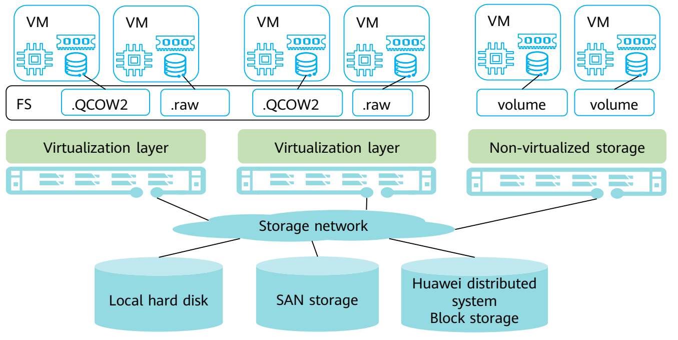
- FusionCompute enables physical server resources to be converted to logical resources. With virtualization technologies, a server can be divided into multiple virtual compute resources that are isolated with each other. CPU, memory, disks, and I/O resources become pooled resources that are dynamically managed. Server virtualization increases the resource utilization, simplifies system management, and implements server integration.
- For end users, VMs can be more rapidly provisioned than physical machines, and their configurations and networking can be more easily modified. For maintenance personnel, the maintenance cost of VMs is significantly lower because hardware is reused by VMs and the cloud platform supports automatic maintenance. For system administrators, the resource usage and change trend are visible so that they can predict expansion requirements.



- FusionCompute enables physical server resources to be converted to logical resources. It divides a server into multiple isolated virtual compute resources, while CPU, memory, disk, and I/O resources become pooled resources that are dynamically managed. This increases the resource utilization and simplifies system management. In addition, the hardware-assisted virtualization technology increases virtualization efficiency and enhances VM security.

FusionCompute Product Functions - Virtualized Storage

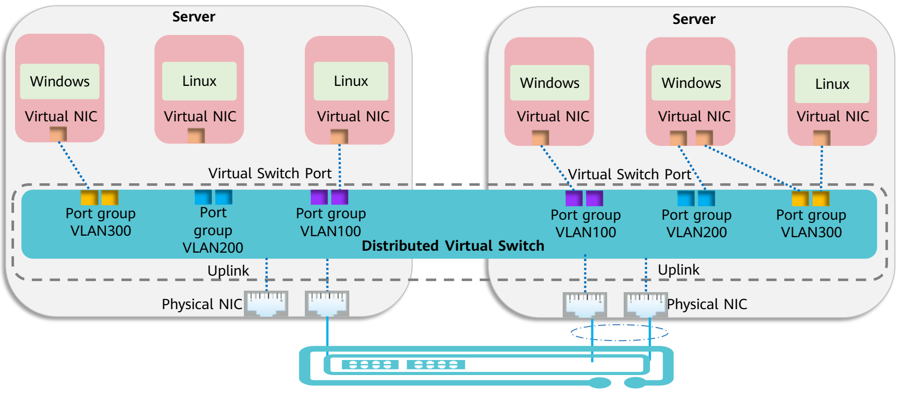
- The storage virtualization technology is used to manage virtual infrastructure storage resources with high resource utilization and flexibility, increasing application uptime. FusionCompute centrally manages the virtual storage resources provided by SAN storage, Huawei Distributed Block Storage, and local disks of compute nodes, and allocates the resources to VMs in the form of virtual volumes.



- Storage devices have different capabilities and interface protocols. The storage virtualization technology can format different storage devices and convert various storage resources into data storage resources for unified management. The storage resources can be used to store VM disks, VM configuration information, and snapshot information. Users manage storage devices in a more homogeneous manner.
- Memory such as VM disks and snapshots are stored in data stores as files. All service operations can be converted into file operations, making operations more intuitive and convenient.
- The storage virtualization platform provides various storage services to improve storage utilization, reliability, maintainability, and user experience
- Huawei provides the host-based storage virtualization function. Users do not need to pay attention to the types and capabilities of storage devices. Storage virtualization abstracts storage devices and presents them as logical resources to provide comprehensive storage services. Provides unified functions for different storage models and device types.
- For end users, you can format, install file systems, install operating systems, and read and write data in the same way as x86 servers use local hard disks. In addition, virtualized storage has the snapshot capability and can be resized, which is not supported by physical disks.
- For administrators, virtual storage volumes are not mapped one-to-one to a specific disk, but converged to several SAN devices. Because the reliability of SAN devices is guaranteed, the workload of replacing hard disks is greatly reduced. In addition, virtual storage has better features than physical disks, such as thin allocation, flexible adjustment, limited QoS, and migration. Therefore, virtual storage has obvious advantages in overall costs.

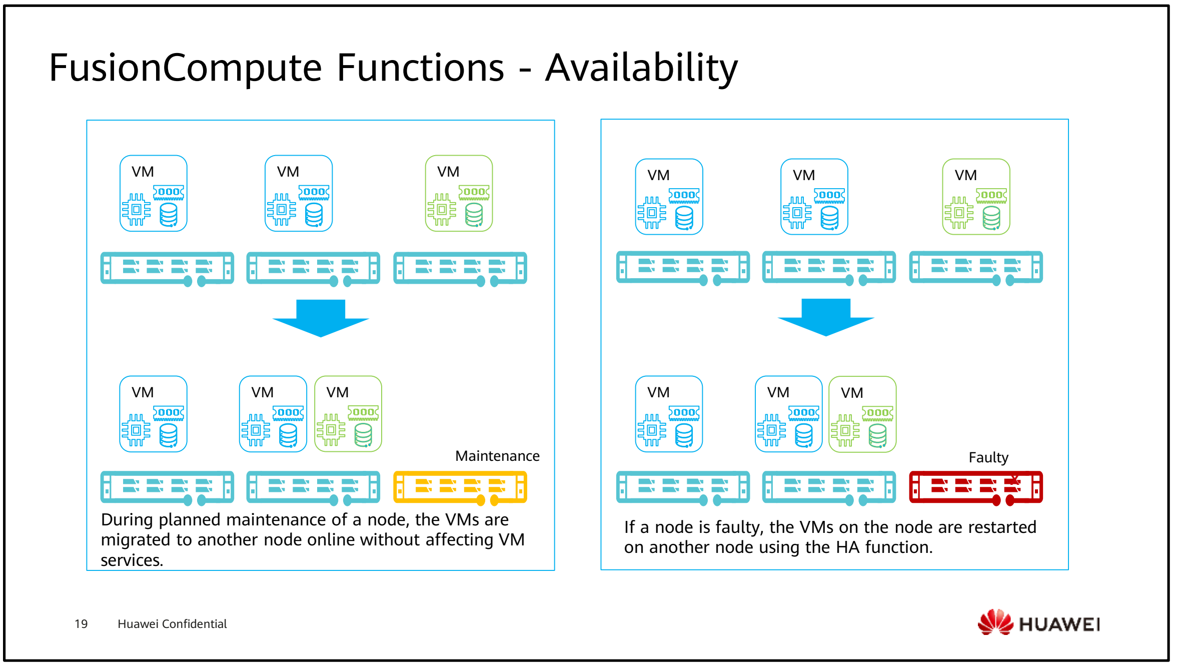
FusionCompute Functions - Virtual Network

- FusionCompute uses distributed virtual switches (DVSs) to provide independent network planes for VMs. Different network planes are isolated by VLANs, like on physical switches.



HUAWEI

- Each virtual NIC (vNIC) has an IP address and a MAC address. It has the same functions as a physical NIC on a network. FusionCompute implements multiple queues, virtual swapping, QoS, and uplink aggregation to improve the I/O performance of virtual NICs.
- The network QoS policy enables bandwidth configuration control, including: Bandwidth control based on the sending direction and receiving direction of a port group member port. raffic shaping and bandwidth priority control for each member port in a port group.
- Each host connects to a distributed virtual switch (DVS), which functions as a physical switch. In the downstream direction, the DVS connects to VMs through virtual ports. In the upstream direction, the DVS connects to physical Ethernet adapters on hosts where VMs reside. The DVS implements network communication between hosts and VMs. In addition, a DVS serves as a single virtual switch to which associated hosts connect. In addition, the DVS ensures unchanged network configuration for VMs when the VMs are migrated across hosts.



- Live migration: In FusionCompute, this feature enables VMs to be migrated from one host to any host across compute clusters. During the migration, services are not interrupted. If the migration fails, the VM on the destination server will be destroyed. The user can still use the VM on the source server. This reduces the service interruption time caused by server maintenance and saves power consumption for data centers.
- Fault-based Migration(HA, high availability): If a VM becomes faulty, FusionCompute automatically restarts the VM. In the process of configuring clusters, the user can enable or disable the HA function. The system periodically checks the VM status. When detecting that the physical server on which a VM runs is faulty, the system will restart the VM on the original physical server or another physical server based on the host fault handling policies so that the VM can be restored in a timely manner. Because the restarted VM will be recreated and loaded with the OS like a physical server, the unsaved data is lost when the VM encountered the error.
- The system can detect errors on the hardware and system software that cause VM failures.

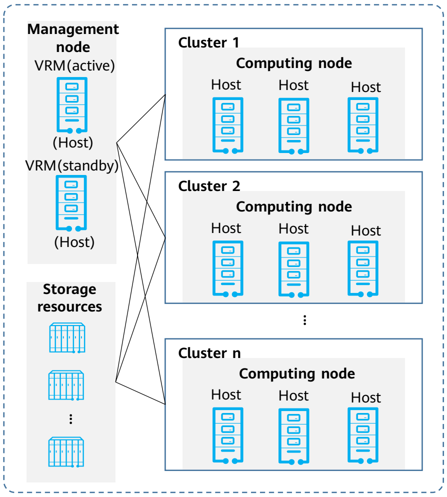
FusionCompute Product Functions - Security

- Virtual Network Access Control
  - The network range of the VMs can be divided by configuring VLAN IDs for VM NICs.
  - The port group to which a VM NIC belongs can be dynamically modified, implementing dynamic modification of VLAN IDs.
  - After the NIC VLAN ID is dynamically changed, the NIC VLAN can also be changed by binding a new VLAN to the NIC without adding a NIC.

- In addition to the virtual network access control in FC, Huawei provides security solutions for different security directions based on the threats and challenges faced by the cloud computing field.
  - Cloud platform security: Data storage security, VM isolation, and network transmission security.
  - O&M management security: Rights management, account security, and log management.
  - Host security: includes web security, SO hardening, database hardening, and security patch.

Contents

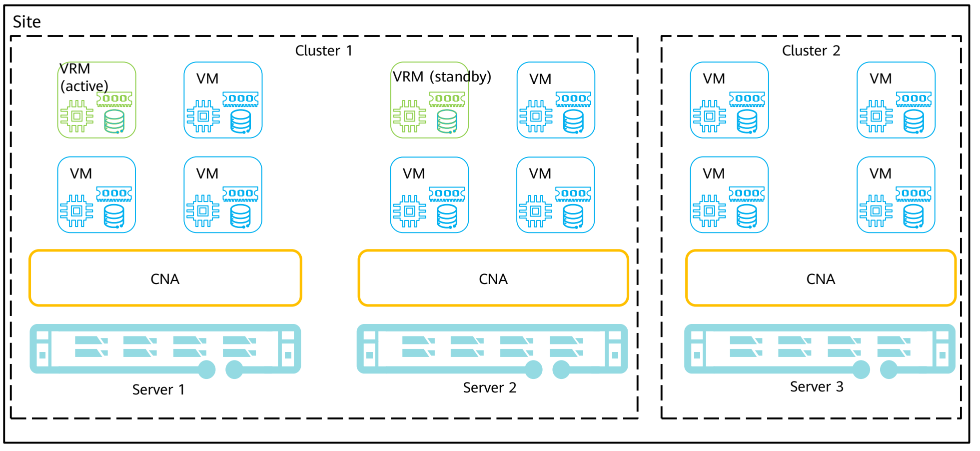
Deployment Plan



Node Type	Deployment Mode	Deployment Rule
Host	Deployed on a physical server	Multiple hosts can be deployed based on customer requirements for compute resources. A host also provides storage resources when local storage resources are used. When VRM nodes are deployed on VMs, a host must be specified for creating a VRM VM. If a small number of hosts (for example, less than 10) are deployed, you can add all the hosts to the management cluster, which therefore also provides user services. If a large number of hosts are deployed, you are advised to add the hosts providing different user services to multiple service clusters to facilitate service management. To optimize compute resource utilization of each cluster, you are advised to configure the same types of data stores and DVSs for hosts in the same cluster.
VRM	Deployed on VMs	The active and standby VRM nodes must be deployed on two VMs on different hosts in the management cluster. You are advised to deploy VRM on VMs.
	Deployed on physical servers	The active and standby VRM nodes must be deployed on different physical servers.

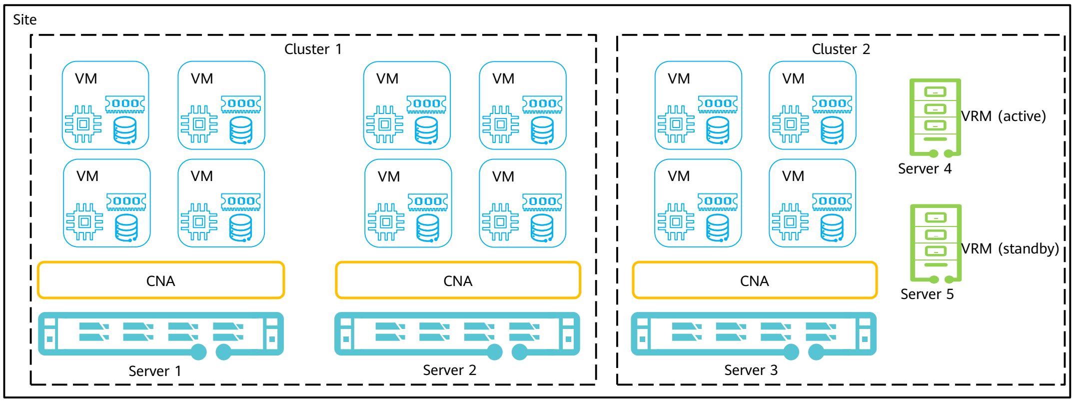
- VRM: FusionCompute management node, which provides a management interface for unified management of virtual resources.
- Host: physical server, which provides computing resources for FusionCompute. When local hard disks are used, the host provides storage resources.

Logical View of VRM Nodes Deployed on VMs



- If the active and standby VRM nodes are deployed on different CNAs, the VRM nodes cannot be migrated after being deployed.
- Cluster1 is a management cluster, and Cluster2 is a computing cluster.

Logical View of VRM Nodes Deployed on Physical Servers

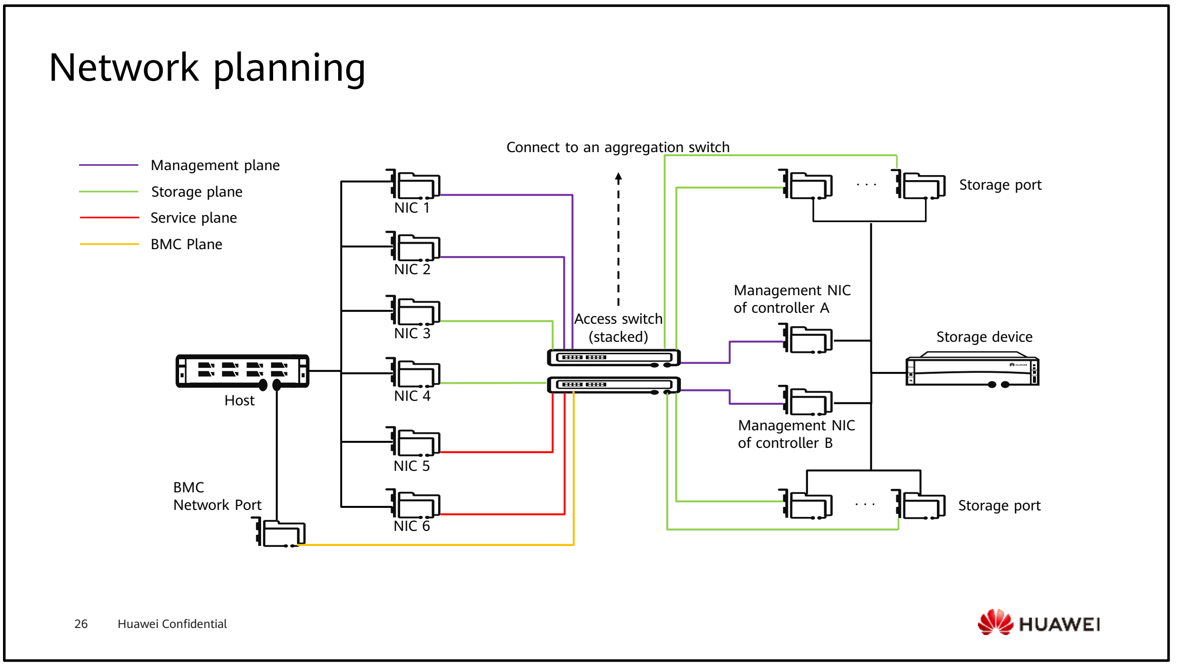


- Active and standby VRM nodes are deployed on different physical servers.

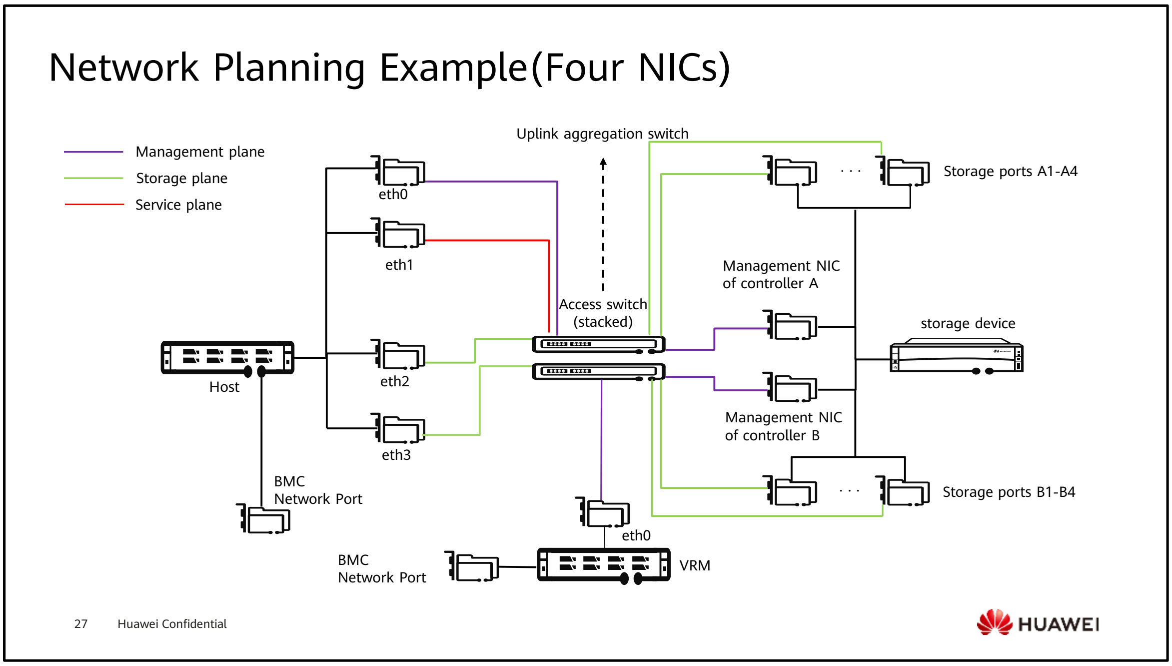
Introduction to the Network Plane

Plane	Description	Network Interoperability Requirements
BMC Plane	Specifies the plane used by the BMC network port on the host. This plane enables remote access to the BMC system of a server.	The management plane and the BMC plane of the VRM node can communicate with each other. The management plane and the BMC plane can be combined.
Management plane	Specifies the plane used by the management system to manage all nodes in a unified manner. All nodes communicate on this plane, which provides the following IP addresses: • Management IP addresses of all hosts, that is, IP addresses of the management network ports on hosts • IP addresses of management VMs • IP addresses of storage device controllers It is recommended that you configure eth0 on a host as the management network port. If a host has more than four network ports, configure both eth0 and eth1 on the host as the management network ports, and bind them to work in active/standby mode after FusionCompute is installed.	The VRM node communicates properly with CNA nodes over the management plane.
Storage plane	Specifies the network plane on which hosts communicate with storage units on storage devices. This plane provides the following IP addresses: • Storage IP addresses of all hosts, that is, IP addresses of the storage network ports on hosts. • Storage IP addresses of storage devices. If the multipathing mode is in use, configure multiple VLANs for the storage plane.	Hosts communicate properly with storage devices over the storage plane. You are not advised to use the management plane to carry storage services, which ensures storage service continuity even when you subsequently expand the capacity for the storage plane.
Service plane	Specifies the plane used by user VMs.	-

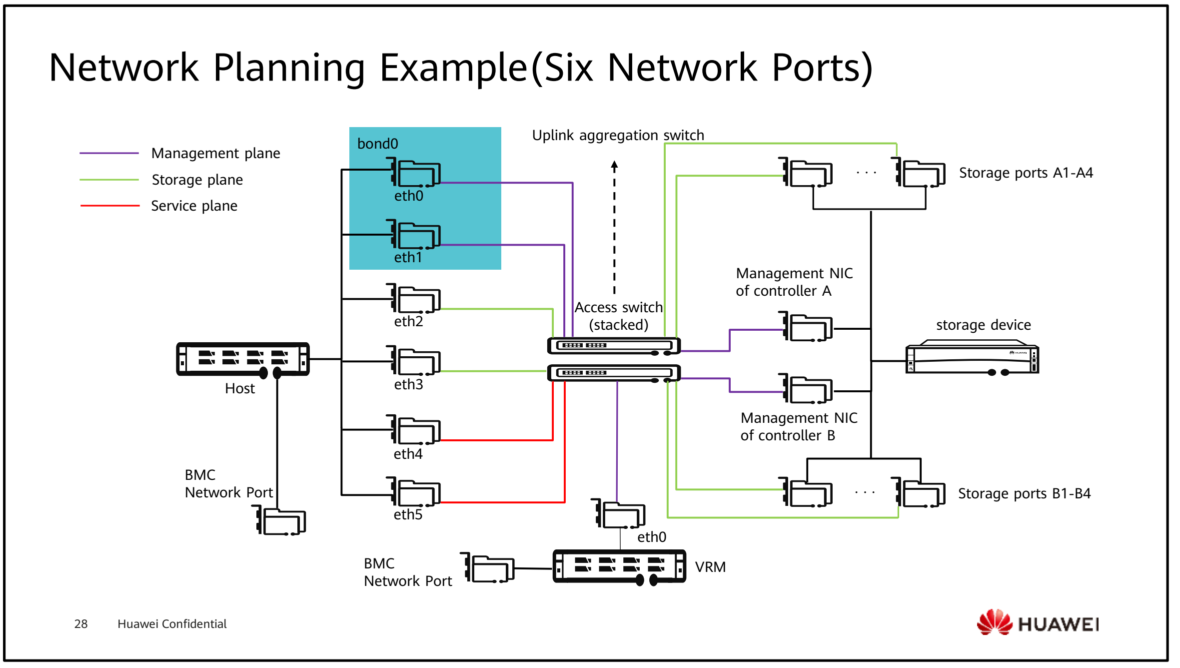
- The Baseboard Management Controller (BMC) network port of each node can be assigned to the BMC plane or the management plane.
- You are advised to bind network ports on different NICs to the same plane to prevent network interruption caused by the fault of a single NIC.
- When binding network ports on different NICs, ensure that the models of the NICs to be bound are the same. If the models of the NICs to be bound are different, bind the network ports on the same NIC.
- The management plane is accessible to the IP addresses in all network segments by default, because the network plans of different customers vary. You can deploy physical firewalls to deny access from IP addresses that are not included in the network plan.
- If you use a firewall to set access rules for the floating IP address of the VRM node, set the same access rules for the management IP addresses of the active and standby VRM nodes.
- On the FusionCompute management plane, some ports provide management services for external networks. If the management plane is deployed on an untrusted network, it is prone to denial of service (DoS) and DDoS attacks. Therefore, you are advised to deploy this management plane on a dedicated network or in the trusted zone of the firewall, protecting the FusionCompute system against external attacks.
- SSH and SFTP ports are high-risk ports. Do not expose the SSH and SFTP ports of the system to the Internet without passing through the firewall. If the preceding services must be exposed to the Internet, take measures



- Based on different service types, a network can be manually divided into multiple network planes by VLAN. Each network plane can be configured with one or more VLANs.
- To ensure networking reliability, you are advised to deploy switches in stacking mode. If NICs are sufficient, you can use two or more NICs for connecting the host to each plane.
- This section assumes the typical internal networking for a host that has six physical NICs deployed and uses IP SAN or Huawei Distributed Block Storage.
- If the number of NICs deployed on the host is less than six, reduce the number of NICs for each network or combine some planes, for example, combine the service plane and the management plane. Then, isolate them logically by VLAN. For example, configure the same physical NIC for the service and management plane and separate the two planes using different VLANs.
- The FusionCompute system consists of the following communication planes:
- Management plane: provides a communication plane to implement system monitoring, O&M (including system configuration, system loading, and alarm reporting), and VM management (such as creating, deleting, and scheduling VMs).
- Storage plane: provides a communication plane for the storage system and storage resources for VMs. This plane is used for storing and accessing VM data (including data in the system disk and user disk of VMs).
- Service plane: provides a plane for NICs of VMs to communicate with external devices.



- The Baseboard Management Controller (BMC) network port of each node can be assigned to the BMC plane or the management plane.
- You are advised to bind network ports on different NICs to the same plane to prevent network interruption caused by the fault of a single NIC.
- When binding network ports on different NICs, ensure that the models of the NICs to be bound are the same. If the models of the NICs to be bound are different, bind the network ports on the same NIC.
- The management plane consists of:
  - Network port eth0 on the host
  - Network port eth0 on the active and standby VRM nodes
  - BMC network ports on the VRM and host
- Storage plane:
  - Storage network ports A1, A2, A3, A4, B1, B2, B3, and B4 on the SAN storage devices
  - Storage network ports eth2 and eth3 on the host
- Service plane:
  - Service network port eth1 on the host



- The management plane consists of:
  - Network ports eth0 and eth1 on the host(bond0)
  - Network port eth0 on the active and standby VRM nodes
  - BMC network ports on the VRM and host
- Storage plane:
  - Storage network ports A1, A2, A3, A4, B1, B2, B3, and B4 on the SAN storage devices
  - Storage network ports eth2 and eth3 on the host
- Service plane:
  - Service network ports eth4 and eth5 on the host

Installation Data Plan

Number type	Parameter	Description	Example
Host information	Host Name	It identifies a server in the system.	CNA01
	Management Plane IP Address	It specifies the IP address of the host management network port.	192.168. 4.10
	Management Plane Subnet Mask/Prefix Length	It specifies the subnet mask or subnet prefix length of the host management plane.	IPv4:255.255.255.0 IPv6:112
	Management Plane Gateway	It specifies the gateway IP address of the host management plane.	192.168. 4.1
	Management plane VLAN (optional)	It specifies the VLAN of the management plane. If no value is specified, the system uses VLAN 0 by default.	2
VRM node information	VRM Node Name	It identifies a VRM node in the system.	VRM01
	Management Plane IP Address	If the VRM node is deployed on a physical server, set this parameter to the IP address of the VRM management network port. If the VRM node is deployed on VMs, set this parameter to the IP address of the VRM VM.	192.168. 4.41
	Management Plane Subnet Mask/Prefix Length	It specifies the subnet mask or subnet prefix length of the VRM management plane.	IPv4:255.255.255.0 IPv6:112
	Management Plane Gateway	It specifies the gateway IP address of the VRM management plane.	192.168. 4.1
	Management plane VLAN	It specifies the VLAN of the management plane. If no value is specified, the system uses VLAN 0 by default.	2
	Floating IP address	The floating IP address of the VRM nodes must be an idle IP address that resides on the same network segment as the management IP addresses of the active and standby VRM nodes.	192.168. 4.30
	Arbitration IP address	The active and standby VRM nodes periodically send a ping command to all arbitration IP addresses. If the active VRM node cannot ping any arbitration IP address, but the standby VRM can ping at least one arbitration IP address, the active and standby switchover is triggered.	192.168. 4.1

- Management Plane IP Address: If the VRM node is deployed on a physical server, this parameter specifies the IP address of the VRM management network port. You are advised to select the management IP address from a private network segment, because a management IP address from a public network segment may pose security risks.If the VRM node is deployed on a VM, it specifies the IP address of the VRM VM. The two VRM nodes must share one management port. You are advised to configure eth0 or bond0 as the management port of the two VRM nodes.
- Floating IP address: This parameter is required only when two VRM nodes are deployed in active/standby mode.
- Arbitration IP address: This parameter is required only when two VRM nodes are deployed in active/standby mode. At most three arbitration IP addresses can be entered. The active and standby VRM nodes periodically send ping commands to all arbitration IP addresses. If the active VRM node cannot ping all arbitration IP addresses and the standby VRM node can ping at least one arbitration IP address, an active/standby switchover is triggered. You are advised to set the first arbitration IP address to the gateway address of the management plane, and set other arbitration IP addresses to the IP addresses of global servers, such as the AD domain server and DNS server, that can communicate with the management plane.

Contents

Installation Preparation (1)

Installation PC or Laptop

- Memory: > 2 GB
- Excluding the partition for the OS, at least one partition has more than 16 GB of free space for installing FusionCompute.
- The local PC can communicate with the planned management plane.
- Google Chrome 85, 87, and 90; Mozilla Firefox 87, 88; Safari 13, 14; Microsoft Edge 85, 87, 90; Opera 74, 75, 76 are supported.

Server CNA

- x86: Intel 64-bit CPU and Hygon 64-bit CPU; Arm: Phytium 64-bit CPU
- The CPU supports the hardware virtualization technology, such as Intel VT-x, and the CPU virtualization function has been enabled in the BIOS.
- Memory > 8 GB; Recommended memory size: ≥ 48 GB;
- System disk of compute nodes: ≥ 150 GB. The system requires two SAS disks to form a RAID1 group. System disk of the service system where the VRM node resides: ≥ 270 GB.

Precautions

- Do not change the IP address of the local PC or laptop during the installation.
- Before installing FusionCompute, ensure that the firewall on the local PC is disabled.
- The folder path cannot contain Chinese characters. The complete path length cannot exceed 256 characters.
- Do not restart the host during environment setup.

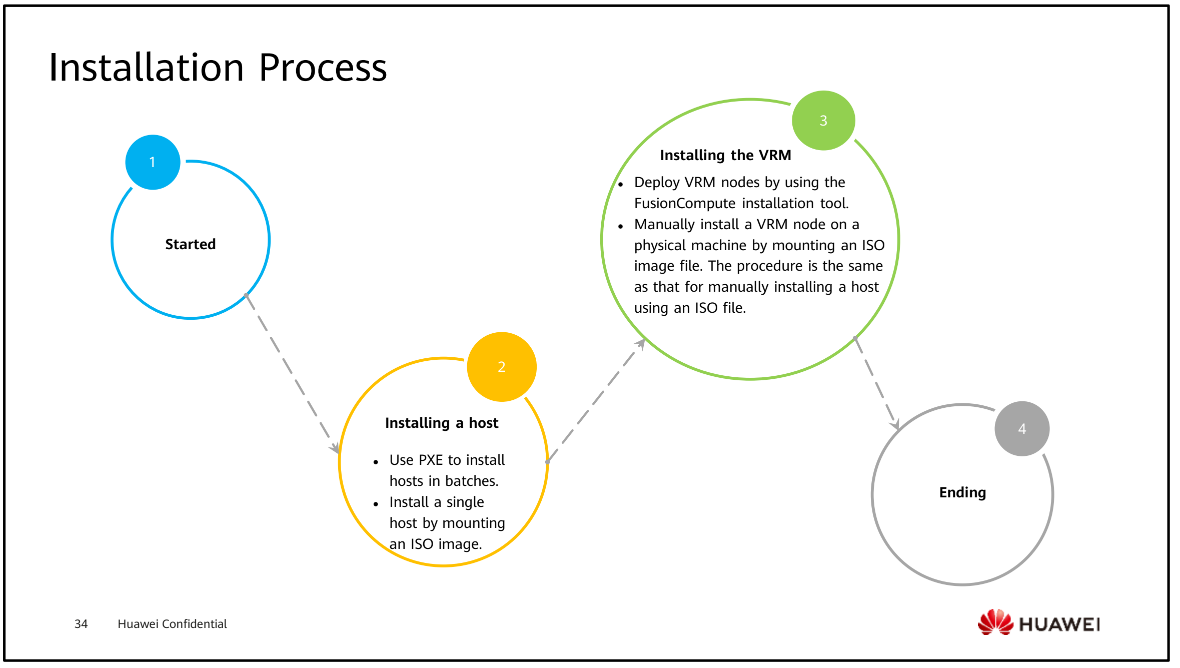
- This section describes only some software and hardware requirements. For details about other configuration requirements, see the product documentation.
- Before installing FusionCompute, ensure that the firewall on the local PC is disabled.
- Before the installation, you need to prepare the local PC, host, storage device, and network environment, and check the physical network environment.
  - Storage device requirements:
    - FusionCompute can be installed only on a local storage device.
    - If local storage resources are used, only available space on the disk where you install the host OS and other bare disks can be used as data store.
    - If shared storage devices are used, including SAN and NAS storage devices, you must configure the management IP addresses and storage link IP addresses for them. A virtual data store provides high performance when it serves a small number of hosts. Therefore, you are advised to add one virtual data store to a maximum of 16 hosts.
  - Network environment requirements:
    - SNMP and SSH must be enabled for the switches to enhance security. SNMPv3 is recommended.
    - The STP protocol must be disabled for the switches. Otherwise, a host fault alarm may be generated incorrectly.
    - To ensure networking reliability, you are advised to deploy switches in stacking mode. If NICs are sufficient, you can use two or more NICs for connecting the host to each plane.

        - The management plane and BMC plane of the VRM node can communicate with each other. The management plane and BMC plane can be combined. The VRM and CNA nodes are on the same management plane and can communicate with each other. All hosts can communicate with the storage plane of the storage device. Do not directly use the management plane as the storage plane. Otherwise, storage services will be interrupted during storage plane expansion.
    - Physical networking requirements:
        - The management network and service network must be isolated.
        - A single aggregation switch or two aggregation switches (in stacking mode) are deployed on the network..
        - A single firewall or two firewalls (active and standby) are connected to the aggregation switch in bypass mode. Virtual firewalls have been created on the in-use firewalls to provide gateways for networks in the VPC.
        - All servers in a cluster are of the same model, and the VLAN settings for all clusters are the same.
- You can download the software package from http://support.huawei.com/enterprise.
- Product documentation link: https://support.huawei.com/hedex/hdx.do?docid=EDOC1100278150&id=EN-US_TOPIC_0000001198673256.

Installation Preparation (2)

Category	Name	Description
Document Preparation	Network Integration Design	Software deployment plan
	Integration Design Data Plan Template	Data planning result
	FusionCompute 8.3.0 Version Mapping	Provides information about the mapping between software and hardware versions.
	FusionCompute 8.3.0 Software Package Download List	Download each software package of FusionCompute before software installation.
Tool Preparation	PuTTY	A cross-platform tool used for accessing nodes on a Windows platform during software installation.
	WinSCP	A cross-platform file transfer tool, which is used to transfer files between Windows and Linux OSs.
Software package	FusionCompute-LinuxInstaller-8.3.0-X86_64.zip	FusionCompute installation tool
	FusionCompute_CNA-8.3.0-X86_64.iso	FusionCompute host OS
	FusionCompute_VRM-8.3.0-X86_64.zip	VRM VM template

- How to obtain:
  - Enterprise users: Log in to https://support.huawei.com/enterprise, search for the software package name and download it.
  - Carrier users: Log in to https://support.huawei.com, search for the software package name and download it.
- After obtaining the software package, do not change the name of the software package. Otherwise, the tool cannot verify the software package when it is uploaded. As a result, the installation fails.



- For details about how to install FusionCompute, see the lab manual. This lab manual uses the FusionCompute web tool installation method to install the lab environment.

Quiz

1. (Multiple Choice) Which of the following products are included in the FusionCompute virtualization suite?
   - A. FusionCompute
   - B. FusionCompute Plus
   - C. eBackup
   - D. UltraVR
2. (Multiple Choice) What are the benefits of FusionCompute?
   - A. Improving resource utilization
   - B. Improve system availability
   - C. Reduced TCO
   - D. Green and energy saving

- Answers:
  - ACD
  - ABCD

Summary

- In this chapter, we have learned the basic concepts, architecture, and positioning of the FusionCompute virtualization platform. We have learned about the functions, planning, and deployment of the FusionCompute virtualization platform. In the next chapter, we will continue to learn about the management and usage of the Huawei FusionCompute.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Abbreviations

- CBT: Changed Block Tracking
- CNA: Compute Node Agent
- VRM: Virtual Resource Management

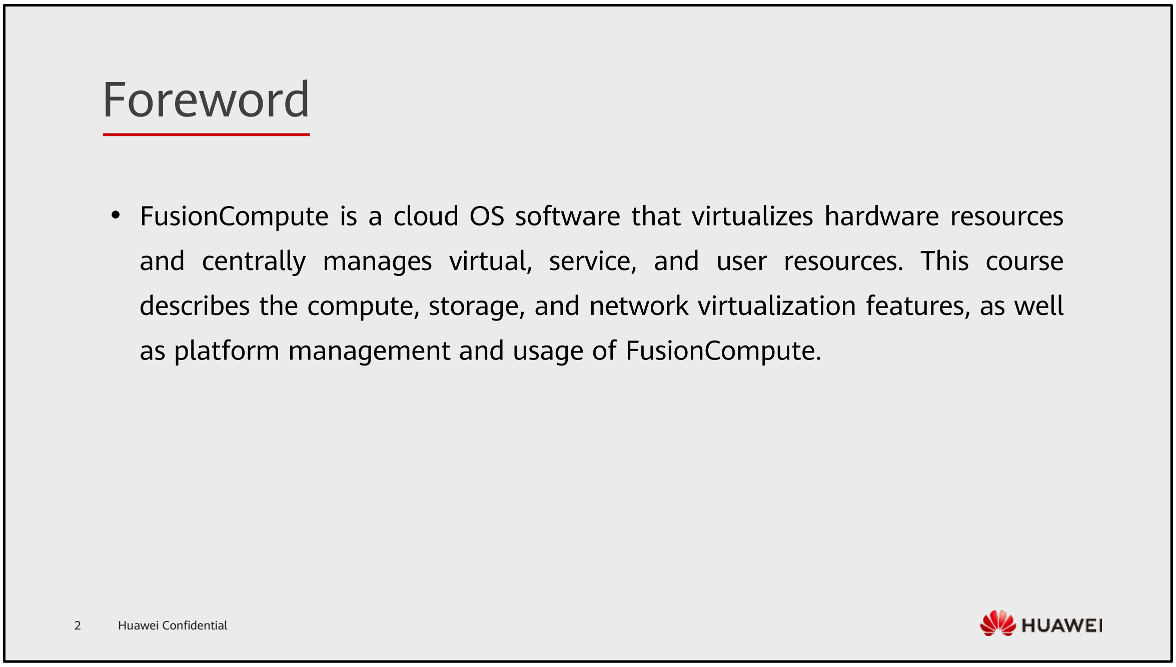
Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

Huawei Virtualization Platform Management and Usage



- FusionCompute is a cloud OS. It virtualizes hardware resources and centrally manages virtual resources, service resources, and user resources. It virtualizes compute, storage, and network resources using the virtual computing, virtual storage, and virtual network technologies. It centrally schedules and manages virtual resources over unified interfaces. FusionCompute provides high system security and reliability, and reduces the OPEX, helping carriers and enterprises build secure, green, and energy-saving data centers.

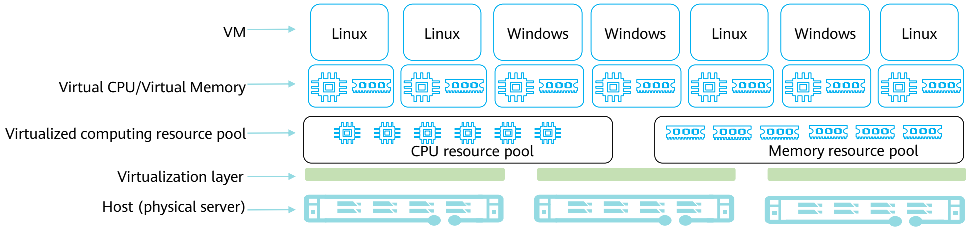
Objectives

- On completion of this course, you will be able to:
  - Understand FusionCompute compute virtualization features.
  - Understand FusionCompute storage virtualization features.
  - Understand FusionCompute network virtualization features.
  - Familiarize yourself with the FusionCompute system and resource management.

Contents

Compute virtualization

- FusionCompute resources include host and cluster resources, network resources, and storage resources.
- The FusionCompute system integrates physical CPUs and memory resources on hosts into a compute resource pool and divides the resources into virtual CPUs and memory resources for VMs.



- Host and cluster management involves the following operations on FusionCompute: creating a cluster or host and adjusting and scheduling host or cluster resources.
- Host (physical server) & virtualization layer: After the FusionCompute host OS is installed on a physical server, compute resources (CPUs and memory) on the physical server can be virtualized, that is, a virtualization layer is generated.
- Virtualized computing resource pool: Virtualized compute resources on hosts are integrated into a compute resource pool. Typically, a compute resource pool contains resources from all hosts in the same cluster.
- Virtual CPU, virtual memory, and VMs: During VM creation, the system automatically allocates required memory space and virtual CPUs from the resource pool to the VM according to the specified VM flavors..
- **Note: The virtual CPU and memory resources used by a VM must be provided by the same host. If this host fails, the system automatically assigns another host to the VM to provide compute resources. Therefore, the resources actually used by a VM cannot exceed the specifications of the hardware resources on the host.**

Compute Virtualization Technologies(1)

- CPU virtualization
  - FusionCompute uses the Kernel-based Virtual Machine (KVM) technology for compute virtualization. KVM is a CPU-based hardware-assisted virtualization solution that requires CPUs to support the virtualization function.
- Memory virtualization
  - The actual physical memory of a physical machine is managed in a centralized mode, and is packed into multiple virtual memories for VMs.
- I/O virtualization
  - I/O virtualization can be considered as a hardware middleware layer between the system of a server component and various available I/O processing units, allowing multiple guest OSs to multiplex limited peripheral resources.

- Key system resources: indicate the registers that affect the status and behavior of processors and I/O devices. System resources include instruction sets and registers for processor access and control and status registers (CSRs) for I/O device access.

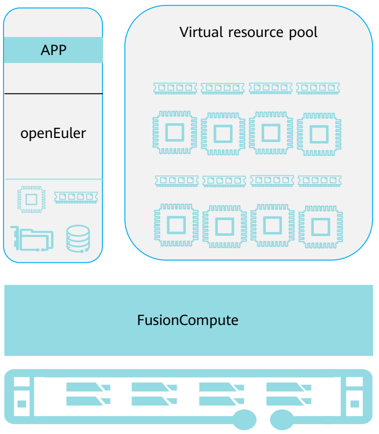
Compute Virtualization Technologies(2)

- Full virtualization
  - The VMM is used to virtualize the CPU, memory, and device I/O. The guest OS and computer system hardware do not need to be modified.
- Paravirtualization
  - The VMM is used to implement CPU and memory virtualization, and the guest OS is used to implement device I/O virtualization. The guest OS needs to be modified so that it can work with the VMM.
- Hardware-assisted virtualization
  - Enable efficient full virtualization with hardware (mainly processors). The guest OS does not need to be modified, and the compatibility is good.

- Full virtualization has good compatibility, but it brings extra overhead to the processor. Paravirtualization has poor compatibility but good performance. Hardware-assisted virtualization will gradually eliminate the differences between software virtualization technologies and become a future development trend.

Contents

VM Resource Management - Online CPU/Memory Adjustment



Technical Principles

- vRAM and vCPUs can be added offline or online and deleted offline.

Technical Features

- CPU and memory specifications can be adjusted when VMs are running. The adjustment takes effect without restarting the VMs.

Application Scenario

- Applies to services that require flexible adjustments to the number of CPUs and memory size of VMs.

Application Value

- Flexibly adjusts VM configuration based on the site requirements.
- Supports scale-up to ensure QoS of each VM.
- Integrates with the scale-out to ensure cluster QoS.

- Supports online CPU and memory size modification for VMs that run a Linux OS.Supports online memory size modification for VMs that run a Windows OS.The online CPU adjustment takes effect after the VMs are restarted.
- If a VM is offline, the number of vCPUs and memory capacity of the VM can be reduced.
- FusionCompute supports adding and deleting NICs and mounting disks offline and online. If a VM is offline or online and uses virtual storage, you can expand the storage capacity of the VM by adding the existing disk capacity.

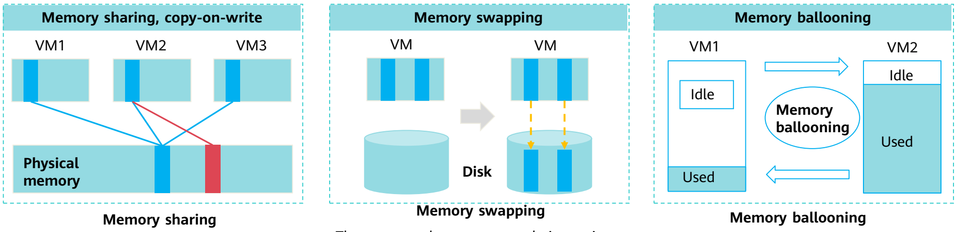
VM Resource Management - CPU QoS

- This feature allows IT administrators to set an upper limit of resources, such as CPUs, memory, networks, and IOPS, available to a VM, preventing non-critical applications or malicious users from preempting shared resources.
- The CPU QoS ensures optimal allocation of compute resources for VMs and prevents resource contention between VMs due to different service requirements. It effectively increases resource utilization and reduces costs.
- During creation of VMs, the CPU QoS is specified based on the services to be deployed. The CPU QoS determines VM computing capabilities. The system ensures the CPU QoS of VMs by ensuring the minimum compute resources and resource allocation priority.

- Quality of Service (QoS): VM CPU QoS is used to ensure VM computing resource allocation, maximize resource reuse, and reduce costs.
- Summary: Computing resources are allocated on demand, competition priorities are optimized, and resource reservation is used to ensure the lowest computing performance, ensuring the performance of mission-critical services.
- CPU QoS consists of the following three parameters:
  - CPU quota defines the proportion based on which CPU resources to be allocated to each VM when multiple VMs compete for the physical CPU resources.
  - CPU reservation defines the minimum CPU resources to be allocated to each VM when multiple VMs compete for physical CPU resources.
  - CPU limit defines the upper limit of physical CPUs that can be used by a VM.

VM Resource Management - Host Memory Overcommitment

- This feature allows a server to provide virtual memory that can be larger than the server's physical memory size using various memory technologies, such as memory ballooning, memory sharing, and memory swapping.



Memory sharing

VMs share the same physical memory space (blue). In this case, the VM only performs read-only operations on the memory.

Replication on write

When the VM needs to write to the memory (red), the VM allocates another memory space and modifies the mapping.

Memory swapping

The memory data not currently in use is swapped and mapped to a disk. When the VM needs to use the memory data, the data is swapped out from the disk back to the memory block.

Memory ballooning

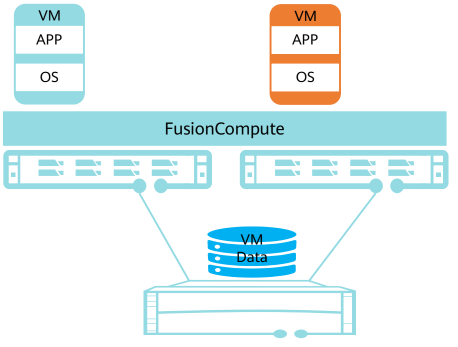
The Hypervisor uses memory bubble to release idle VM memory to VMs with high memory usage, improving memory usage.

With the same memory resources, the VM density is improved and the hardware (memory) procurement cost is reduced by 50%.

- Whether to enable the memory overcommitment technology, which is configurable. Once turned on, all three are turned on.
- Swap volume - Memory switching(Memory swapping): External storage is virtualized into memory for VMs. Data that is temporarily not used by applications on VMs is stored on external storage. When the system needs the data, the system swaps the data with the data in the reserved memory.
- Memory ballooning: The system automatically reclaims the unused memory from a VM and allocates it to other VMs to use. Applications on the VMs are not aware of memory reclamation and allocation. The total amount of the memory used by all VMs on a physical server cannot exceed the physical memory of the server.
- Memory swapping: External storage is virtualized into memory for VMs to use. Data that is not used temporarily is stored to external storage. If the data needs to be used, it is exchanged with the data reserved on the memory.
- Memory sharing: Multiple VMs share the memory page on which the data content is the same.

VM Live Migration

- The live migration feature allows users to migrate VMs in a cluster from one physical server to another without interrupting services.



Technical Features

- Memory compression technology doubles the VM live migration efficiency.
- The location of VM disk data remains unchanged, and only the mapping relationship is changed.

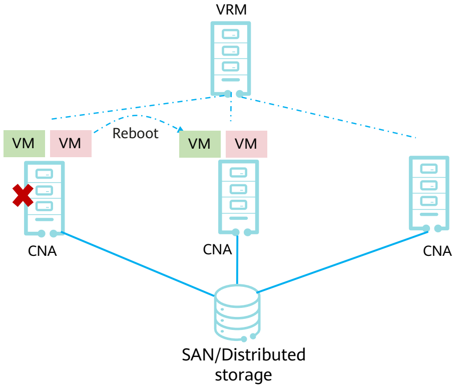
Application Scenario

- Short-term service interruption is tolerated, but services must be recovered quickly. For example, lightweight database services and desktop cloud services.

- This feature allows VMs to be live migrated from one server to another without interrupting user services. The feature applies to planned server maintenance requiring no stop of any user services.
- The VM manager provides quick recovery of memory data and memory sharing technologies to ensure that the VM data before and after the live migration remains unchanged.
- VM live migration is the basis of dynamic resource scheduling and distributed power management technologies.
- Before performing O&M operations on a physical server, system maintenance engineers need to migrate VMs from this physical server to another physical server. This minimizes the risk of service interruption during the O&M process.
- Before upgrading a physical server, system maintenance engineers need to migrate VMs from this physical server to other physical servers. This minimizes the risk of service interruption during the upgrade process. After the upgrade is complete, system maintenance engineers can migrate the VMs back to the original physical server.
- System maintenance engineers need to migrate VMs from a light-loaded server to other servers and then power off the server. This helps reduce service operation costs.

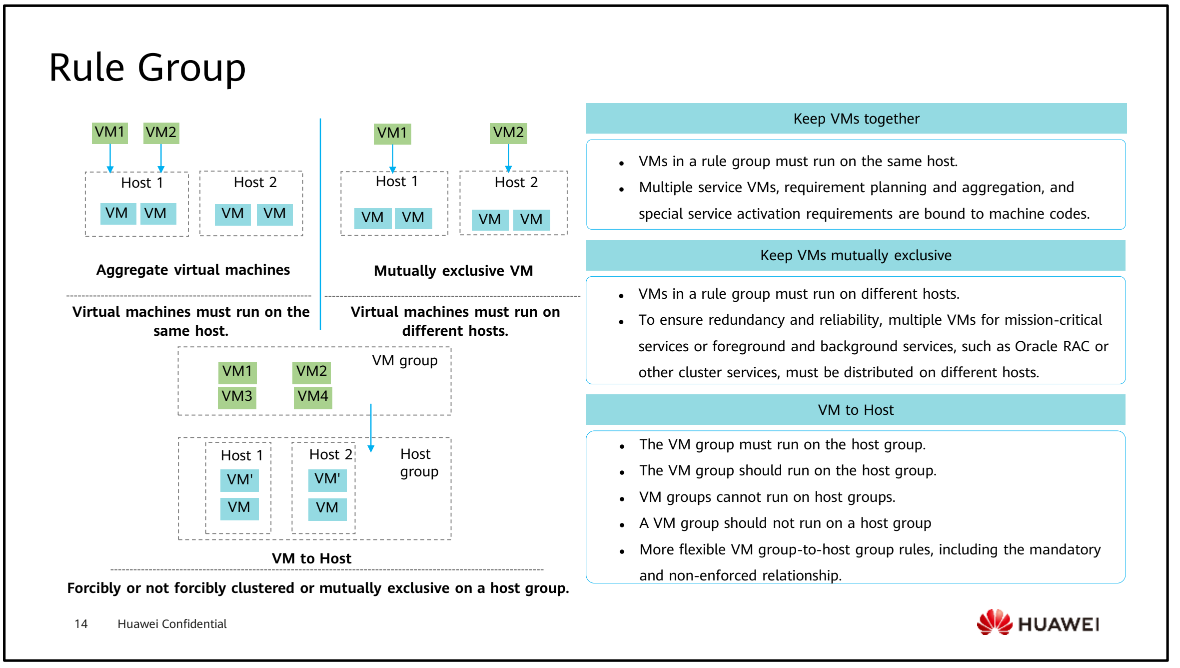
VM HA

- The VM HA feature ensures quick recovery of a VM. With this feature, when a VM is faulty, the system automatically re-creates the VM on another normal compute node.

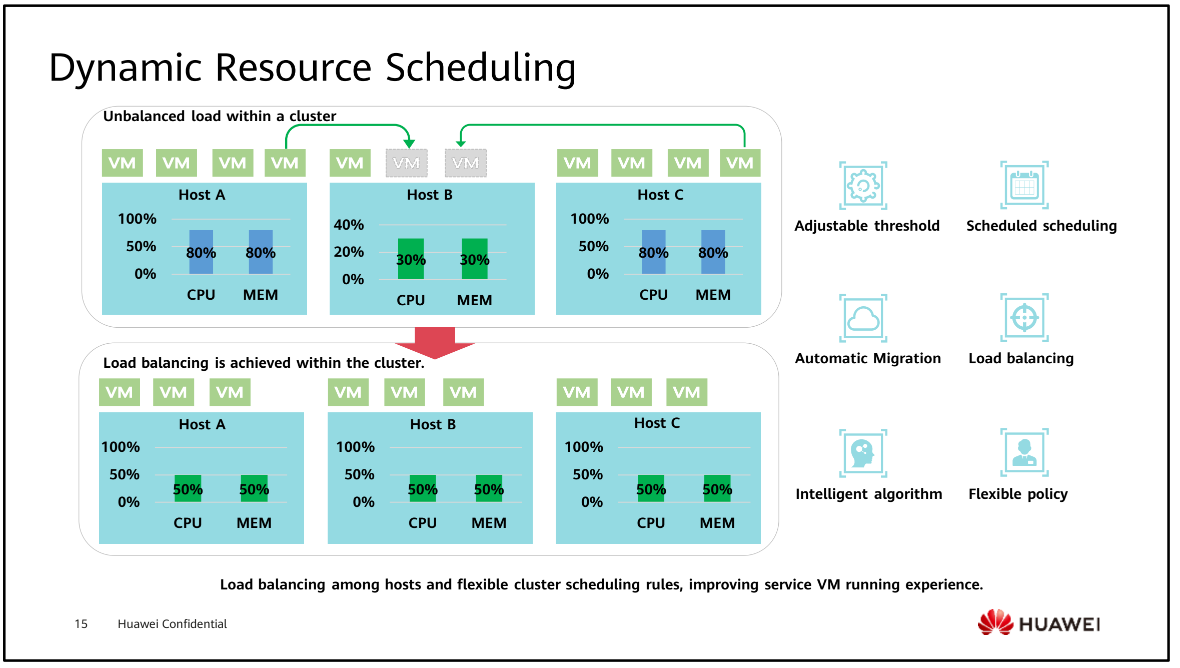


The VM is automatically restored to the new host when an unplanned power failure occurs on the host where the VM resides.

- Supports fault detection and VM recovery in multiple scenarios of hosts, virtual platforms, and VMs.
- Supports centralized HA and cluster-autonomous HA.
- The network plane for HA heartbeat messages can be configured to reduce the network pressure.
- Multiple fault judgment mechanisms are used to avoid missing or misjudgment of faults.
- Supports shared storage and local storage VM HA.
- Restart or restoration of a compute node from a power failure: When a compute node restarts or recovers from a power outage, the system re-creates the HA VMs running on this node on other compute nodes.
- VM blue screen on display (BSOD) (x86 architecture: When detecting that BSOD occurs on a VM and the handling policy configured for this error is HA, the system re-creates the VM on other normal compute nodes.



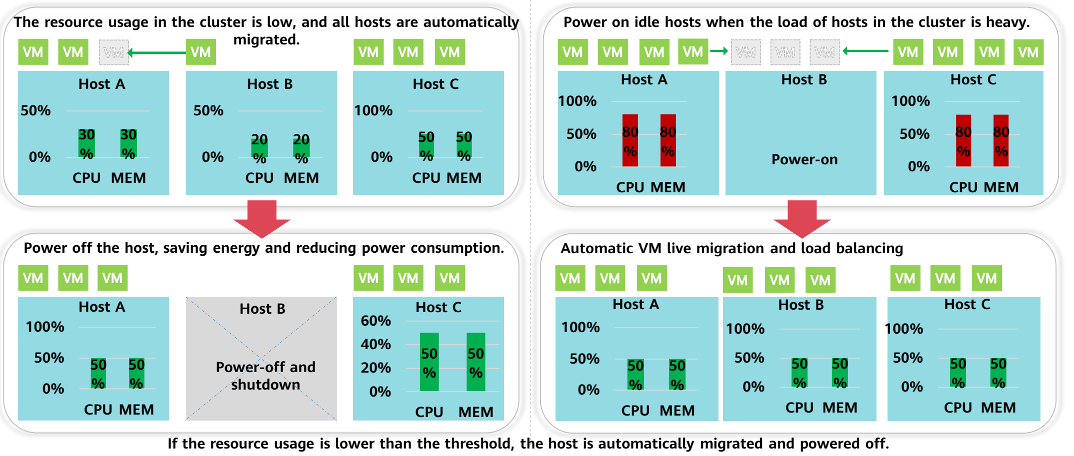
- Rule groups can be used to control the location relationships between VMs and between VMs and hosts to meet the requirements of different application scenarios.
- **Keep VMs together**: This rule keeps the selected VMs always running on the same host. One VM can be added to only one keep-VMs-together rule group.
- **Keep VMs mutually exclusive**: This rule keeps the selected VMs running on different hosts. One VM can be added to only one VM-mutually-exclusive rule group.
- **VMs to hosts**: This rule associates a VM group with a host group so that the VMs in the specified VM group can be configured to run only on the specified host in the host group.
- **VMs to VMs**: Set the dependency between the two VM groups and specify the low-priority VM groups to depend on the high-priority VM groups. When VMs are started in batches, VMs in the high-priority VM group are started first.



- Dynamic Resource Schedule (DRS) uses intelligent scheduling algorithms to periodically monitor the work load on hosts in a cluster and migrates VMs between the hosts based on the work load to achieve load balancing. This feature collaborates with the dynamic power management (DPM) to increase resource utilization and reduce power consumption.
- FusionCompute monitors global resource usages during VM creation and running. In the monitoring process, FusionCompute uses an intelligent resource scheduling algorithm to determine the optimal host on which the VMs can run, and it also migrates the VMs to this optimal host by means such as live migration, ensuring VM stability and improving user experience.
- FusionCompute computing cluster, which works with the shared storage based on the VIMS file system; The DRS algorithm monitors the resource usage of each computing node in the cluster in real time and uses the VMOTTION function to intelligently migrate VMs from heavily loaded nodes to nodes with sufficient resources. Balances resource usage on each node and ensures sufficient resources for services. Therefore, DRS is the basis for implementing automatic load balancing.
- When the system is lightly loaded, the system migrates some VMs to one or more physical hosts and powers off the idle hosts.
- When the system is heavily loaded, the system starts some VMs and physical hosts and allocates VMs evenly on hosts to ensure resource supply.
- Scheduled tasks can be set to enable different resource scheduling policies at different times based on the system running status to meet user requirements in different scenarios.

- Dynamic resource scheduling does not take effect on the following types of VMs:
  - A VM that has been bound to a host
  - A VM that has been bound to a USB flash drive
  - A VM that has been bound to a passthrough device
  - A VM that has been bound to GPU resource group

Dynamic Power Management



If the resource usage is lower than the threshold, the host is automatically migrated and powered off.

When the resource usage exceeds the threshold, the host is automatically powered on to achieve load balancing.

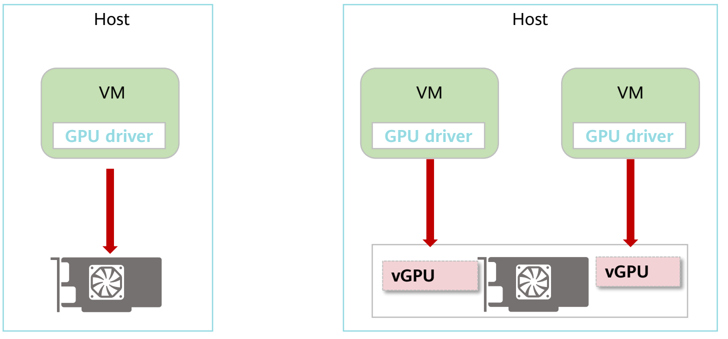
HUAWEI

- Dynamic power management, also known as automatic power management, periodically checks the resource usage of servers in the cluster. If resources in the cluster are sufficient but service load on each host is light, the system migrates VMs to other hosts and powers off these hosts to reduce power consumption. If the in-service hosts are overloaded, the system powers on offline hosts in the cluster to balance load among hosts.
- When the automated power management function is enabled, automated compute resource scheduling must be enabled so that the system automatically balances VM load on hosts after the hosts are powered on.
- The time-based power management settings allow the system to manage power in different time periods based on service requirements. When services are running stably, set automated power management to a low level to prevent adverse impact on services.
- With the automated power management function enabled, the system checks resource usage in the cluster, and powers off some light loaded hosts only when the resource utilization drops below the light-load threshold over the specified time period (40 minutes by default). Similarly, the system powers on some hosts only when the resource utilization rises above the heavy-load threshold over the specified time period (5 minutes by default). You can customize the time period for evaluating the threshold of powering on or off hosts.

- Technical features:
  - The system automatically selects a proper physical machine to power off the system to reduce the number of VMs to be migrated.
  - Ensure that a small number of physical machines are in the dormant state to quickly meet the requirements of new services.
- Application scenario:
  - Automatically migrate VMs and power off idle hosts when the load is low at night.
  - When the service requirements increase during the daytime, the host is automatically powered on and VMs are migrated to the newly powered-on host.

GPU passthrough and GPU virtualization

- FusionCompute supports GPU passthrough and GPU virtualization, improving high-performance graphics and image application experience.



GPU passthrough

GPU virtualization

- GPU passthrough: A GPU on a physical server can be directly attached to a specified VM to improve graphics and video processing capabilities. With this feature enabled, the system can meet user requirements for high-performance graphics processing capabilities..
- GPU virtualization(Intel): GPUs on an x86 physical server can be virtualized into multiple vGPUs used by multiple VMs based on the hardware technology. GPUs provide the VMs with 2D graphics processing and 3D graphics rendering acceleration services and feature high performance and low costs. In this way, the GPUs are shared and user costs are lowered.

Contents

Introduction to Storage Virtualization

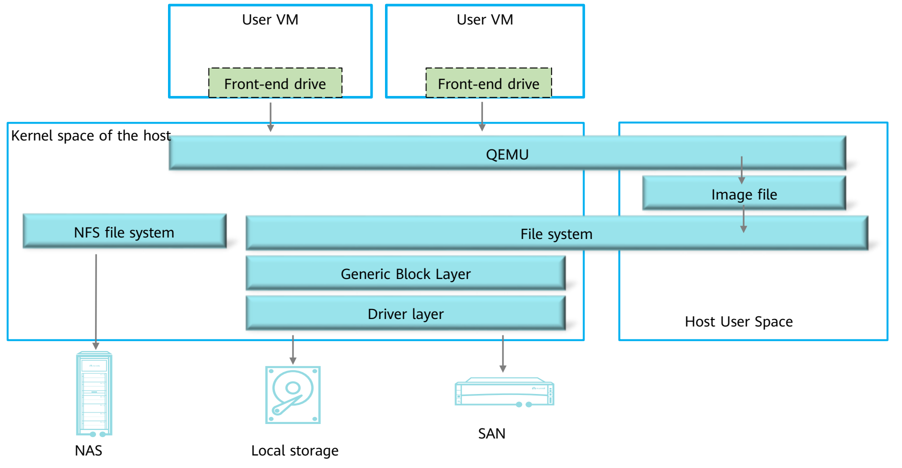
- Storage virtualization abstracts storage devices to datastores so that each VM can be stored as a group of files in a directory on a datastore. A datastore is a logical container that is similar to a file system. It hides the features of each storage device and provides a unified model to store VM files. Storage virtualization better manages the storage resources for virtual infrastructure, significantly improving the storage resource utilization rate and flexibility.

Storage Concepts in FusionCompute

- Storage resources
  - Local disk of the host
  - Dedicated storage devices, such as SAN storage, NAS storage, OceanStor Pacific, OceanStor 6.X, and OceanStor Dorado 6.X.
- Storage Devices
  - A storage device is a management unit in storage resources, such as LUNs, storage pools on Huawei distributed block storage, and NAS shared directories.
- Datastore
  - FusionCompute uniformly transforms storage units of storage resources into datastores.
- Storage resources that can be converted to datastores are:
  - LUNs on SAN devices, including iSCSI storage devices and FC SAN storage devices
  - File systems on NAS devices
  - Storage pools on Huawei distributed block storage
  - Local hard disks (virtualization) on hosts
  - Storage pool on the eVol storage

- FusionCompute can use storage resources provided by dedicated storage devices or local disks on hosts. Dedicated storage devices are connected to hosts through network cables or fiber cables.
- After storage resources are converted to datastores and associated with hosts, virtual disks can be created for VMs.
- A storage pool is a container for storing storage space resources. All storage space used by application servers comes from the storage pool.
- As for the VM OS, the virtual disks created on different storage resources are the same. The usage mode is the same as that of the physical PC.
- FusionCompute is a highly competitive virtualization platform for telecom service environments. It provides security hardening, function expansion, performance optimization, and reliability assurance for open-source KVM. It has the following features:
  - Storage device compatibility: For different storage devices, such as IP SAN, FC SAN, NAS, and local disks, File systems can be used to shield services and provide file-level service operations in a unified manner.
  - Rich functions: provides the following functions: thin provisioning, incremental snapshot, cold and live storage migration, linked clone, and VM disk capacity expansion.
  - Homogeneous service capabilities: Services are performed at the virtualization layer. All storage devices provide the same capabilities. There is no special requirement for storage devices.

FusionCompute Storage Virtualization Architecture



- The FusionCompute storage virtualization platform consists of file systems, disk drivers, and disk tools. Block devices, such as SAN devices and local disks, are connected to servers. The block device driver layer and generic block layer offer an abstract view of the block devices and present a single storage device to hosts.
- File systems are created on storage devices that can be accessed by hosts. To create a file system, the host formats storage devices, writes metadata and inode information about the file system to the storage devices, establishes mappings between files and block devices, and manages the block devices, including space allocation and reclamation. The file system eases operation complexity by making operations on block devices invisible. VM disks are files stored in the file system.
- The disk driver attaches disks to VMs only when the VMs need to use their disks. The VMs are managed through the machine emulator QEMU. The read and write I/O is received by a front-end driver, forwarded to the QEMU process, converted to read and write operations in the user-mode driver, and then written into disk files.
- Attributes and data blocks are included in VM disks. The disk tool can be used to perform VM disk-related operations, including parsing disk file headers, reading and modifying disk attributes, and creating data blocks for disks.

FusionCompute datastore Usage

01 Virtualized storage

- Datastores can be virtualized. Creating a common disk on a virtual datastore takes a long time. However, the virtualized datastore supports some advanced feature, such as creating thin provisioning disks. It also supports more advanced features to improve storage utilization and system security and reliability.
- Formatting: When a storage device is added as a datastore for the first time, ensure that the data on the storage device has been backed up or is not used any longer and set Format to Yes. In this case, the system formats the storage device to be used as the Huawei virtual file system.

02 Non-virtualized storage

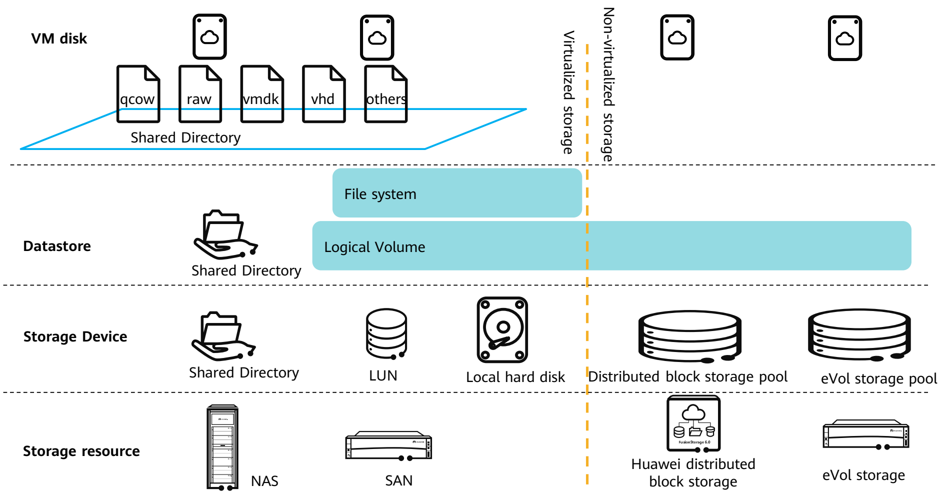
- If the storage resource is Huawei distributed block storage or eVol, the datastore is not virtualized by default.

03 Raw device mapping

- Physical LUNs of SAN storage can be attached to service VMs as disks, improving SAN storage performance.

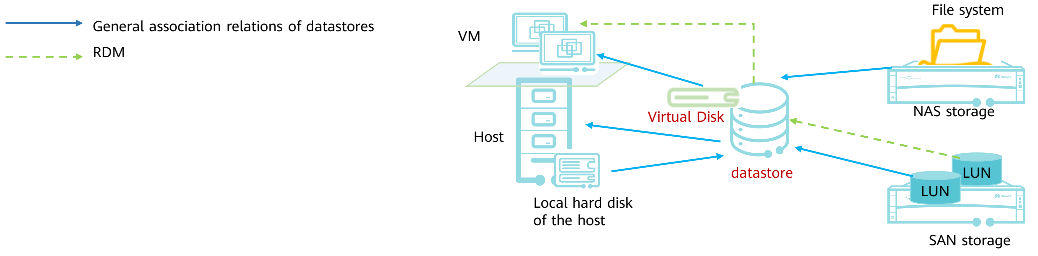
- The datastore of the RDM can be used as the entire disk of the RDM. Therefore, only disks with the same capacity as the datastore can be created and advanced functions of virtualized storage are not supported.

Storage model in FusionCompute



- When adding a datastore to a local hard disk, you can select the virtualization mode.
- When adding a datastore to the SAN, you can select the virtualization and raw device mapping modes.
- Huawei distributed block storage uses the non-virtualized mode by default when data storage is added.

Data Storage Association Model

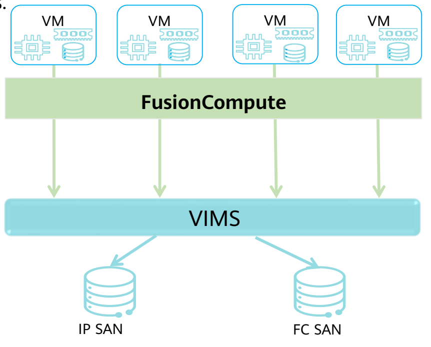


Storage Device	Storage Resources	Datastore
Local disk	N/A	Virtualized local disks (virtualization)
SAN device (IP SAN or FC SAN)	SAN	Virtualized SAN storage (virtualized) RDW (raw device mapping)
NAS storage	NAS storage	NAS storage
Huawei distributed block storage	Huawei distributed block storage	Huawei distributed block storage
eVol storage	eVol storage	non-virtualized

- Table describes the relationship between storage resources, storage devices, and datastores.

VIMS Virtual Cluster Storage File System

- The virtual image management system (VIMS) that enables the application of the virtualization technology to exceed the limit of a single storage system. It enables multiple VMs to access an integrated clustered storage pool, greatly improving resource utilization. The Virtual Image Management System (VIMS), as the basis for virtualizing multiple storage servers, provides services such as live migration, Dynamic Resource Scheduler (DRS), and high availability for storage devices.



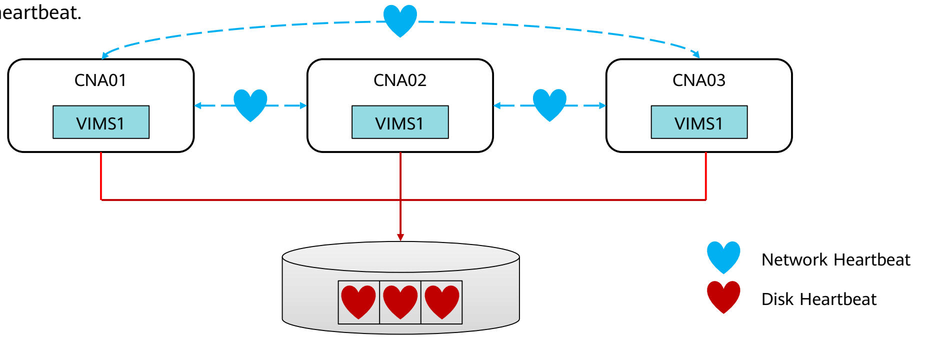
- The virtual image management system (VIMS) is a high-performance cluster file system. datastores are first formatted into the VIMS format to provide file-level service operations.
- Datastores support the following file system formats:
    - Virtual Image Management System (VIMS): A high-performance file system optimized for storing virtual machines. Hosts can deploy virtual image management system data storage on any SCSI-based local or networked storage device, including Fiber Channel, fiber Channel over Ethernet, and iSCSI SAN devices.
    - Network File System (NFS): A file system on a NAS device. FusionCompute supports the NFS V3 protocol. Users can access and mount NFS disks on NFS servers to meet storage requirements.
    - EXT4: FusionCompute supports local disk virtualization.
- Key capabilities of VIMS:
    - High-performance file system optimized for storing virtual machines
    - Shielding storage device differences and reusing heterogeneous or existing storage devices
    - Physical storage devices are managed and scheduled in pools, significantly improving resource utilization.

VIMS Distributed Lock

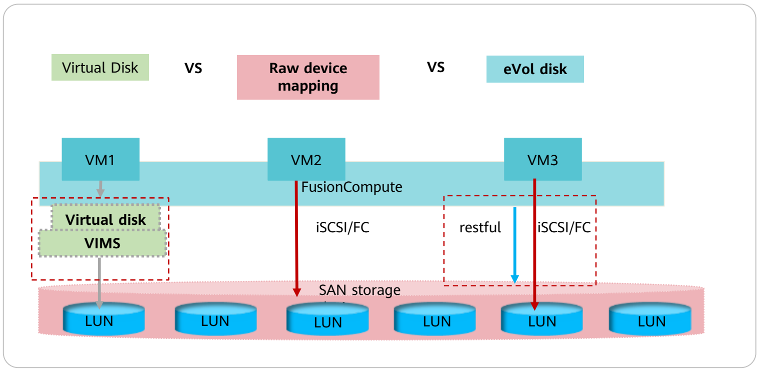
- A VIMS volume is mounted to multiple CNA nodes at the same time. Therefore, each CNA node can access files on the VIMS volume. To ensure data consistency when multiple nodes read and write the same file, the VIMS needs to implement distributed file lock. The DLM (Distribute lock manager) module of the VIMS is responsible for implementing distributed file locks. It provides the lock service in the cluster concept. The invoker uses the DLM to ensure the synchronization between clusters.
- The VIMS uses the distributed full symmetric lock mechanism. There are multiple resource managers (masters) in the VIMS, and each master corresponds to only one lock resource. Different master nodes are not centralized on the same node. There is no management center node.
- In normal cases, you can become the master of a lock resource in either of the following modes:
  - First node that applies for accessing a resource
  - If multiple nodes access a resource at the same time, the node with a smaller VIMS node ID is used as the master node. nodes access a resource at the same time, the node with a smaller VIMS node ID functions as the master node.
- When a node is faulty, the resources managed by the node will be re-elected as the master.

VIMS Heartbeat

- The VIMS has two types of heartbeats. The disk heartbeat is used to check whether the host can read and write the shared storage, and the network heartbeat is used to check whether the network communication between hosts is normal. As a cluster file system, the CNA node mounted with the VIMS volume is not an independent individual. As a cluster node member, the CNA node ensures normal network communication with other nodes through the network heartbeat.



eVol Storage

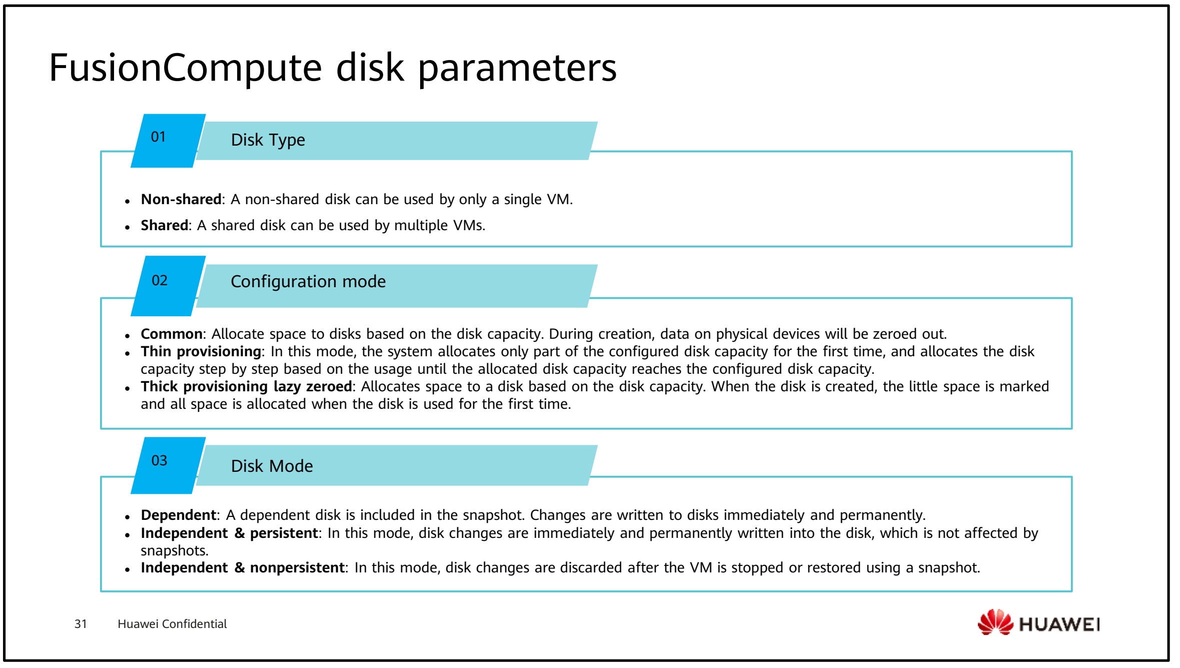


Shorten storage device I/O paths, provide ultimate performance, and enable end-to-end provisioning automation and storage offloading.

Scenario: high I/O storage, low latency, automatic service provisioning, high performance of virtualized service operations, such as cluster file system and video and image processing, and computing storage.

HUAWEI

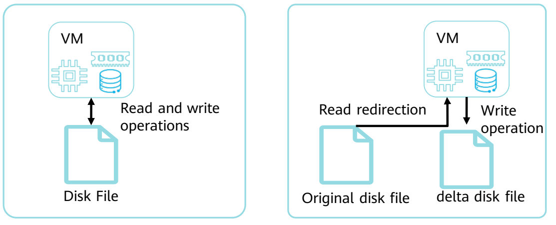
- The eVol storage (originally Advanced SAN storage) uses a storage pool of a storage array as the datastore of FusionCompute. When a disk is created on FusionCompute, a LUN is automatically created on the storage array and virtualized into a virtual disk of a VM.
- eVol storage does not use VIMS for storage virtualization. Therefore, LUN resources do not need to be planned.
- eVol storage offloads various storage management operations, such as VM disk provisioning, reclamation, capacity expansion, snapshoting, clone, and migration, to storage arrays..
- eVol supports OceanStor Dorado V6 series and OceanStor 2910.



- Configuration mode:
  - Common: The system allocates disk space based on the disk capacity. During disk creation in this mode, data remaining on the physical device will be zeroed out. The performance of the disks in this mode is better than that in the other two modes, but the creation duration may be longer than that required in the other modes.It is recommended that system disks use this configuration mode.
  - Thin provisioning: In this mode, the system allocates part of the configured disk capacity for the first time, and allocates the rest disk capacity based on the storage usage of the disk until the configured disk capacity is allocated.
  - Thick provisioning lazy zeroed: The system allocates disk space based on the disk capacity. However, data remaining on the physical device is zeroed out only on first data write from the VM as required. In this mode, the disk creation speed is faster than that in the Common mode, and the I/O performance is medium between the Common and Thin provisioning modes. This mode is supported only when the datastore type is virtualized local disks or virtualized SAN storage.

Delta Disk

- A delta disk must be created based on an existing parent disk. It records only the differential data, including data additions and changes, relative to the parent disk. A delta disk cannot exist separately from the parent disk. If the parent disk is modified, the data on the delta disk is no longer available.
- This disk is used for the snapshot, non-persistent disk, and linked clone functions in the FusionCompute system. It protects the source disk from being modified and traces the differential data on VM disks.



Common disk read/write

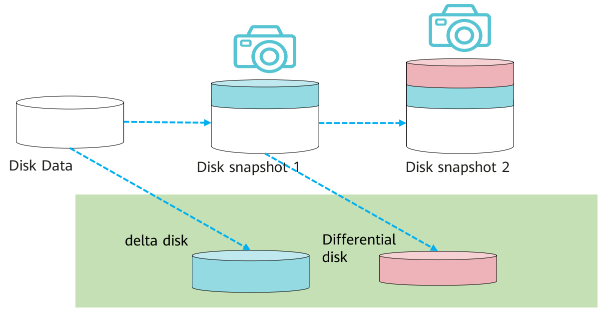
Differential disk read/write

- When a data area on a delta disk is read, the data area on the delta disk is first read. If the data area does not exist, it indicates that the data area is not modified. In this case, the parent disk is found based on the index in the file header, and then the data area is read. When the data is written to the delta disk, the data is directly written to the delta disk.
- The structure of a delta disk is the same as that of a dynamic disk. The file header records the path of the parent disk, and the data area records only the differential data between the delta disk and the parent disk. The size of the delta disk increases automatically as data is written.
- Delta disks cannot be expanded.

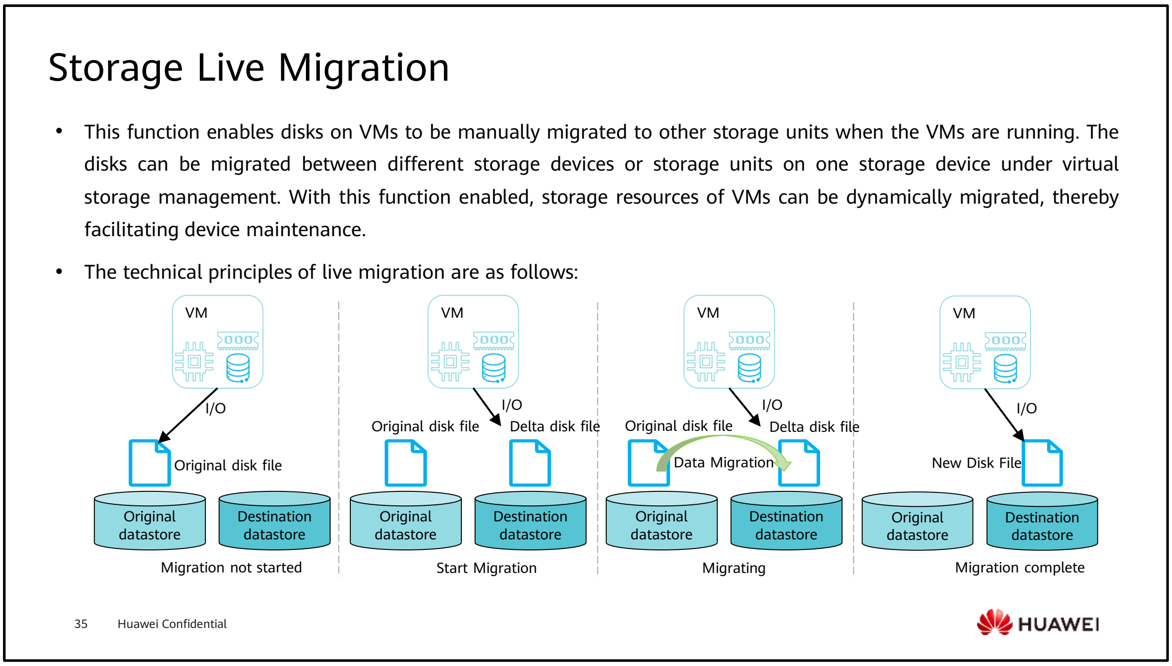
Contents

Snapshot

- A snapshot preserves the VM status and data, including disk, memory, and register data. Users can repeatedly revert the VM to any previous states by use of a snapshot. Before performing critical operations, such as system patch installation, upgrade, and, destructive tests, VM users are advised to take snapshots for quick restoration.
- FusionCompute supports common snapshot, consistency snapshot, and memory snapshot.



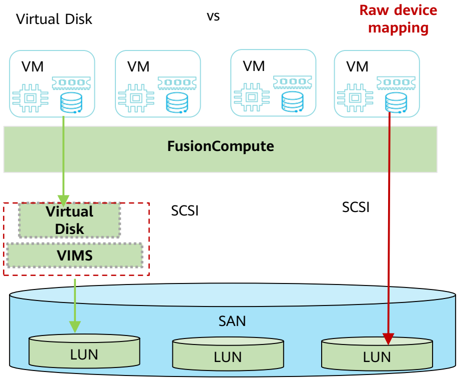
- When a snapshot is created, a delta disk file is created. The delta disk file and the source disk file are stored in the same directory. The source disk file becomes read-only, and the newly written data is stored in the delta disk file.
- When a snapshot is rolled back, the data in the delta disk file is deleted.
- When a snapshot is deleted, the system integrates the data in the original disk and delta disk files to form a new disk file.
- If a snapshot is taken for a VM, all existing disks on the VM become read-only and the system creates a delta disk for each existing disk in the datastore where the read-only disks are created. All disk changes are stored in the delta disks. If a second snapshot is taken for the VM, the created delta disks become read-only and the system creates the second delta disk for each existing disk (despite of the existing delta disk).



- FusionCompute offers cold migration and live migration for VM disks. Cold migration moves VM disks from one datastore to another when the VM is stopped. Live migration moves VM disks from one datastore to another without service interruption.
- In live migration, write-on-write redirection is used to write VM data to a differential disk of the target storage. In this way, the original disk files become read-only.
- All data blocks in the source volume are read and merged into the differential disk on the target end. After the data is merged, the differential disk on the target end has all the latest data on the virtual disk.
- Remove the dependency of the target snapshot on the source volume and change the delta disk to a dynamic disk. In this way, the target disk files can run independently.
- Dependency:
  - Shared disks that have been attached to VMs and disks on a linked clone VM cannot be migrated.
  - A VM in the Running state does not allow non-persistent disks to be migrated. You need to migrate disks after stopping VMs if permitted.
  - Data cannot be migrated between Huawei Distributed Block Storage resources.

RDM of Storage Resources

- Raw device mapping (RDM) provides a mechanism for VMs to directly access LUNs on physical storage subsystems (only through Fiber Channel or iSCSI). By using physical device mapping, VMs can identify SCSI disks.

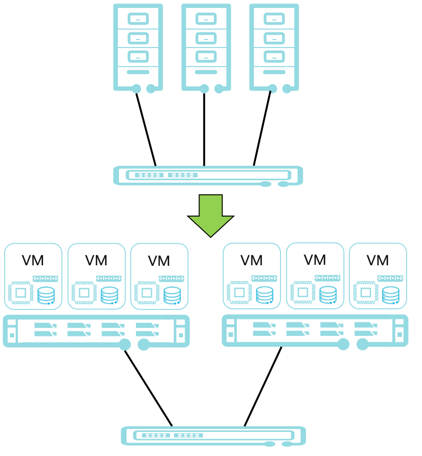


- RDM can bypass a hypervisor layer to transparently transmit the SCSI commands issued by VMs to physical SCSI devices, avoiding function loss due to virtualization layer simulation.
- Advantages of raw device mapping: Shorten the I/O path of storage devices, provide I/O performance close to that of physical storage devices, and support SCSI command transparent transmission.
- Storage thin provisioning, online/offline disk capacity expansion, incremental storage snapshot, iCache, storage live migration, storage QoS, disk backup, and VM template conversion are not supported.
- Technical features:
  - VMs directly issue SCSI commands to operate raw devices.
  - FC SAN storage and IP SAN storage support the RDM feature.
- Applies to applications that require high-performance storage, such as Oracle RAC, cluster file system, and video and image processing services that require high-I/O and low-latency storage.

Contents

Development of Network Virtualization

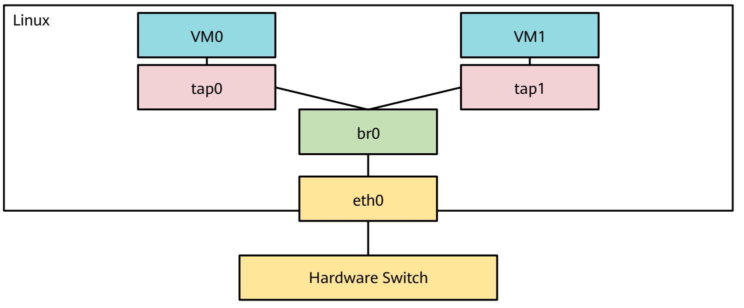
- Compute virtualization stimulates the network virtualization. In traditional data centers, a server runs an OS, connects to a switch through physical cables, and implements data exchange with different hosts, traffic control, and security control using the switch. After compute virtualization is performed, one server is virtualized to multiple virtual hosts and each virtual host has its own virtual CPU, memory, and network interface card (NIC). It is essential for virtual hosts on a single server to maintain communication, while sharing of physical equipment calls for new security isolation and traffic control. This created the demand for the virtual switching technology.
- Distributed virtual switches (DVSs) are used to configure and manage virtual switches on each host in unified and simple manner,. A DVS can configure, manage, and monitor the virtual switches of multiple servers, and ensure network configuration consistency when VMs are migrated between servers.



HUAWEI

Introduction to Linux Bridge

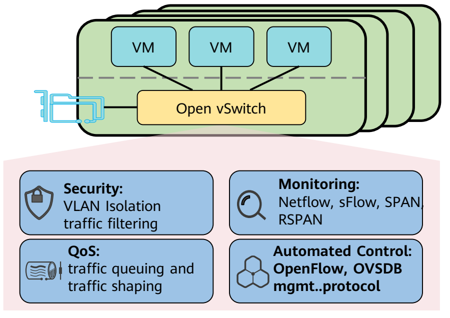
- A Linux bridge is a virtual network device that works at layer 2 and functions like a physical switch.
- A bridge can bind other Linux network devices and virtualize them as ports. Binding a device to a bridge is equivalent to that a network cable connected to a terminal is inserted into the physical switch port.

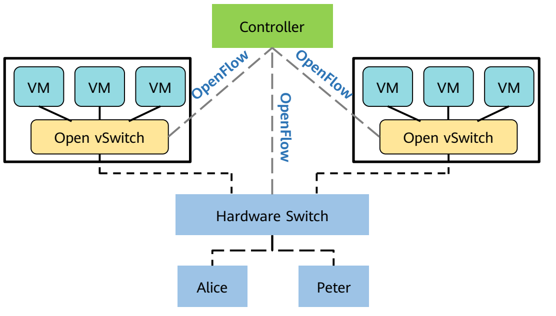


- The bridge **br0** binds the physical device **eth0** and the virtual devices **tap0** and **tap1**. In this case, the upper-layer network protocol stack knows only **br0** and does not need to know bridging details. When receiving a data packet, these bound devices will send the data packet to **br0** for forwarding based on the mapping between the MAC addresses and ports.

Introduction to OVS

- Open vSwitch (OVS) is a software-based open source virtual Ethernet switch.
- It supports multiple standard management interfaces and protocols and supports a distributed environment across multiple physical servers.
- It supports the OpenFlow protocol and can be integrated with multiple open-source virtualization platforms.
- It can be used to transmit traffic between VMs and implement communication between VMs and the external network.

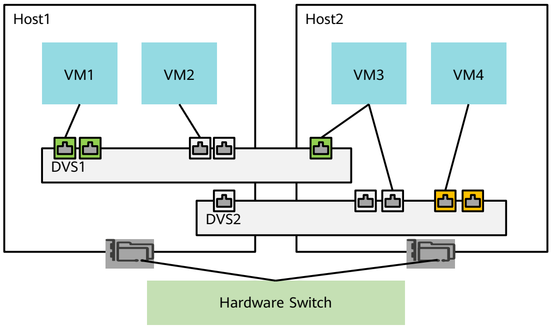




- An Open vSwitch (OVS) is a software-based open-source virtual switch. It complies with the Apache 2.0 license. It supports multiple standard management interfaces and protocols, such as NetFlow, sFlow, SPAN, Remote Switched Port Analyzer (RSPAN), Command Line Interface (CLI), LACP, and 802.1ag. It can be deployed across multiple physical servers (similar to VMware's vSwitch and Cisco's Nexus 1000V). The OVS supports the OpenFlow protocol and can be integrated with multiple open-source virtualization platforms.
- OpenFlow is one of the software-defined networking (SDN) standards. It was first proposed by Professor Nick McKeown of Stanford University in OpenFlow: enabling innovation in campus networks, a paper published in ACM SIGCOMM Computer Communication Review in April 2008. OpenFlow was designed for network researchers to run experimental architectures and protocols in the desired network with no need of modifying the network device in it. It separates the control from the forwarding so that researchers can program the device through a group of clearly-defined interfaces.
- An OpenFlow switch transforms a packet forwarding process controlled originally and entirely by a switch/router into a process completed by the OpenFlow switch and a controller collectively, thereby separating the data forwarding and routing control. The controller controls a flow table on the OpenFlow switch through an interface specified in advance, thereby controlling data forwarding.
- The OpenFlow network includes an OpenFlow switch, a FlowVisor, and a Controller. The OpenFlow switch performs forwarding on a data layer; the FlowVisor virtualizes the network; and the Controller controls the network in a centralized manner and implements functions of a control layer.
- The OpenFlow switch includes three parts: a flow table, a secure channel, and an OpenFlow protocol.

Introduction to DVS

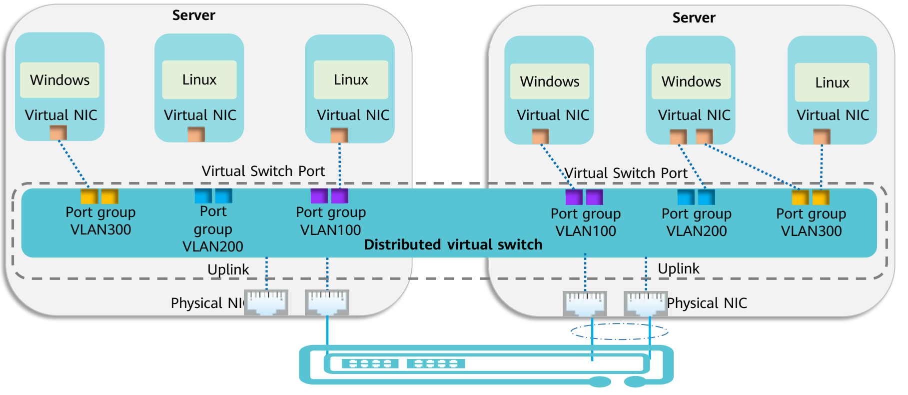
- A distributed virtual switch (DVS) functions as a physical switch and connects to each host. In the downstream direction, a DVS connects to VMs through virtual ports. In the upstream direction, the DVS connects to physical Ethernet adapters on hosts where VMs reside. With such connections established, the host and the VMs running on it can communicate with each other through the DVS. In addition, a DVS functions as a single virtual switch between all associated hosts. This function ensures network configuration consistency during cross-host VM migration.



- DVS: Distributed Virtual Switch

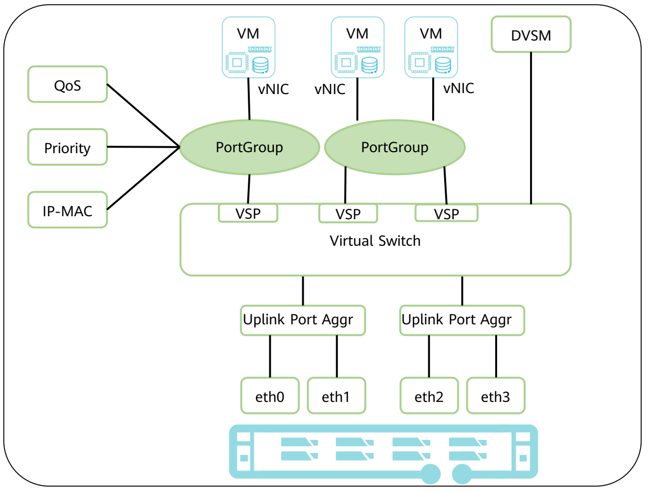
FusionCompute DVS

- FusionCompute uses DVSs to provide independent network planes for VMs. Different network planes are isolated by VLANs, like on physical switches.



- The virtual switch on each physical server provides VMs with capabilities, such as layer-2 communication, isolation, and QoS.
- The DVS model has the following characteristics:
    - Multiple DVSs can be configured, and each DVS can serve multiple CNA nodes in a cluster.
    - A DVS provides several virtual switch ports (VSP) with their own attributes, such as the rate. The ports with the same attributes are assigned to a port group for management. The port groups with the same attributes use the same VLAN.
    - Different physical ports can be configured for the management plane, storage plane, and service plane. An uplink port or an uplink port aggregation group can be configured for each DVS to enable external communication of VMs served by the DVS. An uplink aggregation group comprises multiple physical NICs working based on load-balancing policies.
    - Each VM provides multiple virtual NIC (vNIC) ports, which connect to VSPs of the switch in one-to-one mapping.
    - A server allowing layer-2 migration in a cluster can be specified to create a virtual layer-2 network based on service requirements and configure the VLAN used by this network.
- Concepts related to Huawei distributed switches include the uplink, port group, and VLAN pool.

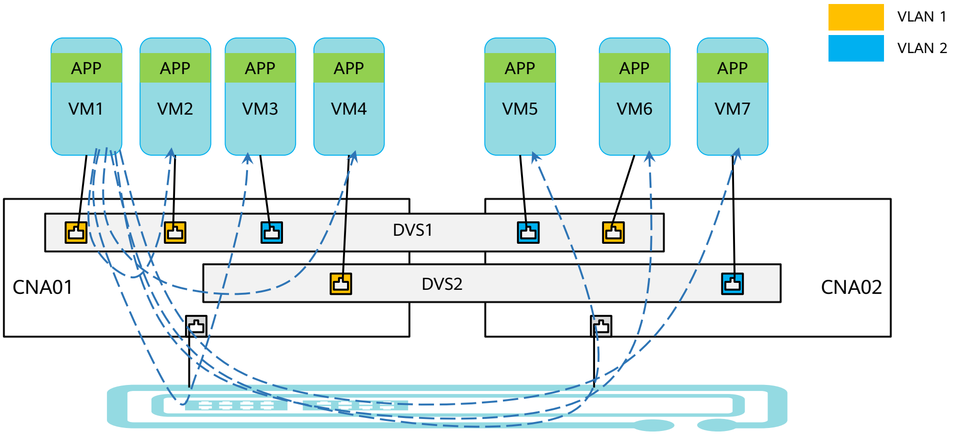
Virtual Switching Model



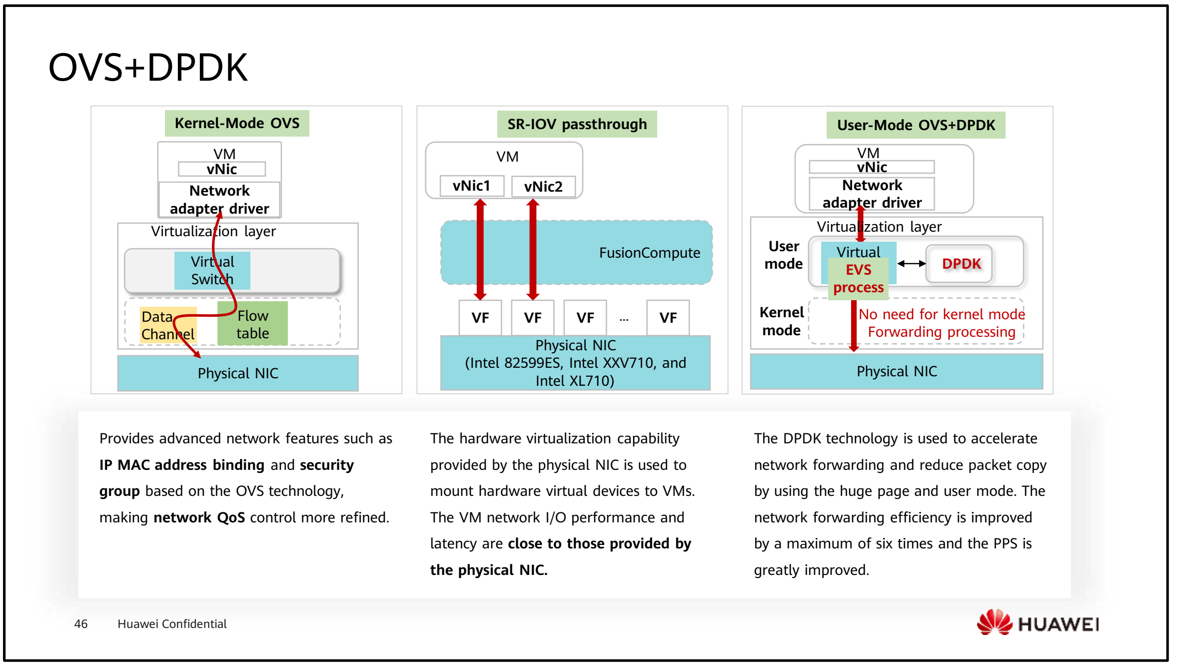
HUAWEI

- DVSM: Distributed Virtual Switch Manager
- Administrators can define port group attributes (security/QoS) to simplify the setting of VM port attributes. Setting the port group attributes does not affect the running of the VM.
- Port group: A port group is a group of ports with the same network attributes.
- Uplink: The link between the DVS and the physical NIC of the host. It is used for VM data uplink.
- Uplink aggregation: The bound network ports of the servers associated with the DVS can contain multiple physical network ports, which can be configured with active/standby or load balancing policies.

VM communication on FusionCompute



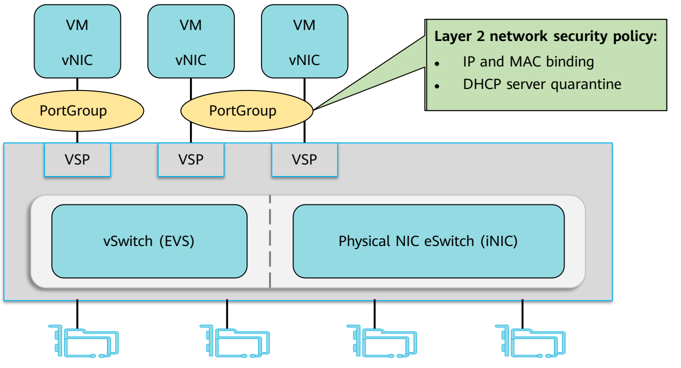
Contents



- By using the DPDK (Data Plane Development Kit is a collection of libraries and drivers.) technology for fast packet processing on x86 platforms. It uses multiple technologies, such as bypassing the kernel protocol stack at the environment abstraction layer, uninterrupted packet sending and receiving in polling mode, optimized memory/buffer/queue management, and load balancing based on NIC multi-queue and flow identification, to achieve high-performance packet forwarding capabilities under the x86 processor architecture. Improves VM network performance.
- The user-mode switching mode supports the following NIC models: Intel 82599ES, Intel XL710, Intel X710, and Mellanox MT27712A0.
- To use the user-mode switching mode, you need to configure the host hugepage memory and user-mode switch specifications of the host first.
- SR-IOV enables PCI functions to be allocated to multiple virtual interfaces to share resources of a PCI device in a virtualized environment. SR-IOV allows network transmission to bypass the software emulation layer and directly allocate to VMs. This reduces the I/O overhead in the software emulation layer. If the VM uses SR-IOV-enabled vNICs, the following functions cannot be used: hibernation, wakeup, online migration, full migration, memory snapshot, memory hot add, online NIC addition and deletion, IP and MAC address binding, and security group.
- SR-IOV mode supports Intel 82599ES, Intel XXV710, Intel X710, and Intel XL710 NICs. Each NIC supports a maximum of 63 virtual network ports.

Layer 2 Network Security Policy

- The layer 2 network security policies are the policies for preventing IP or MAC address spoofing and DHCP server spoofing for user VMs.



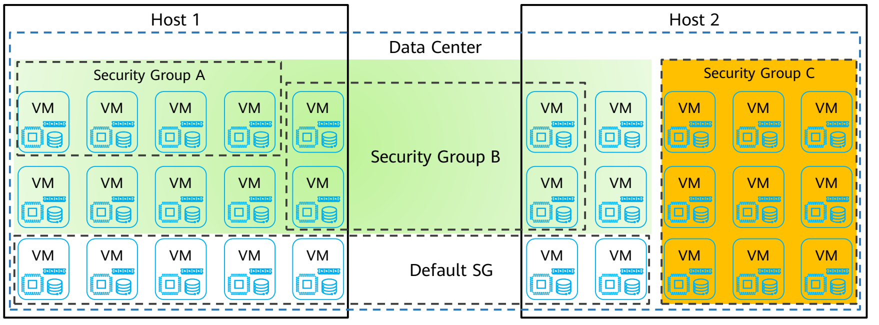
- IP-MAC address binding prevents IP address or MAC address spoofing initiated by changing the IP address or MAC address of a virtual NIC (vNIC), and therefore enhances network security of user VMs. After the binding, the packets from untrusted sources are filtered through IP Source Guard and dynamic ARP inspection (DAI).
- DHCP server quarantine blocks users from unintentionally or maliciously enabling the DHCP server service for a VM, ensuring common VM IP address assignment.

Broadcast Packet Suppression

- In server consolidation and desktop cloud scenarios, broadcast packet attacks caused by network attacks or virus may interrupt network communication. To prevent this, broadcast packet suppression is enabled for virtual switches.
- Virtual switches support suppression of broadcast packets sent from VM ports and suppression threshold configuration. You can enable the broadcast packet suppression switch of the port group where VM NICs locate and set thresholds to reduce Layer 2 bandwidth consumption of broadcast packets.
- The administrator can log in to the system portal to configure the packet suppression switch and packet suppression threshold for port groups of a virtual switch.

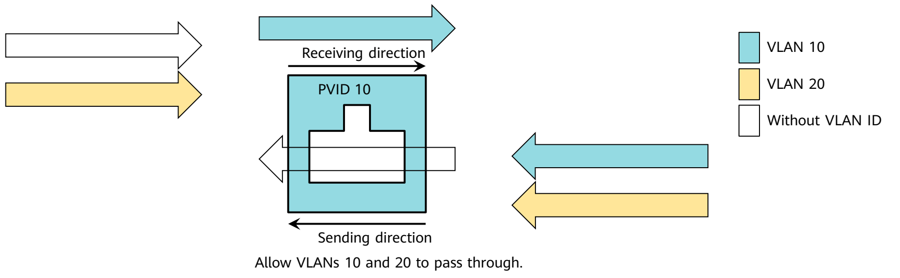
Security group

- Users can create security groups based on VM security requirements. A set of access rules can be configured for each security group. VMs that are added to a security group are protected by the access rules of the security group. Users can add VMs to security groups for security isolation and access control when creating VMs.



- All VM NICs in the same security group use the security group rule for network communication. A VM NIC can be added to only one security group.

Trunk Port

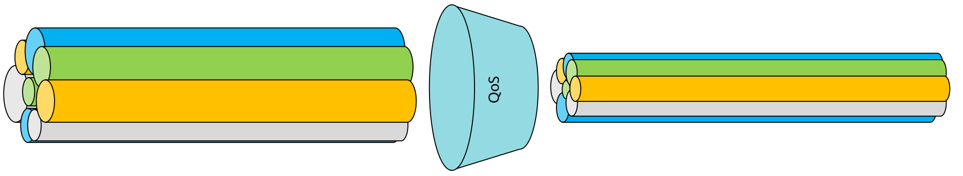


Trunk port overview

- A vNIC communicates with a virtual switch through virtual ports.
- vNIC ports can be configured as virtual trunk ports to send and receive network data packets tagged with specified VLAN IDs.

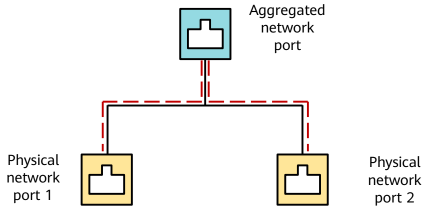
- An access port can be added to only one VLAN. A trunk port can receive and send packets from multiple VLANs. Select **Access** for a common VM, and select **Trunk** if a VLAN device is used for the VM NIC. Otherwise, the VM network may be disconnected.
- If the ports added to a port group are set to the trunk mode on a Linux VM, multiple VLAN tagging devices can be created on the VM to transmit data packets from different VLANs over one vNIC, exempting the VM from using multiple vNICs.

Network QoS



Network QoS policies provide the following bandwidth configuration and control capabilities:
• Bandwidth control based on the sending and receiving directions of a port group member port. • Provides traffic shaping and bandwidth priority control based on each member port in a port group.

Network Port Binding



Host Network Port Binding
• Administrators can use FusionCompute to bind network ports on CNA hosts to improve network reliability. • Port binding can be configured for common NICs and physical NICs driven by DPDK.

- The following binding modes are available for common NICs:
  - Active-backup
  - Round-robin
  - IP address and port-based load balancing
  - MAC address-based load balancing
  - MAC address-based LACP
  - IP address-based LACP
- The following binding modes are available for DPDK-driven NICs:
  - DPDK-driven active/standby
  - DPDK-driven LACP based on the source and destination MAC addresses
  - DPDK-driven LACP based on the source and destination IP addresses and ports

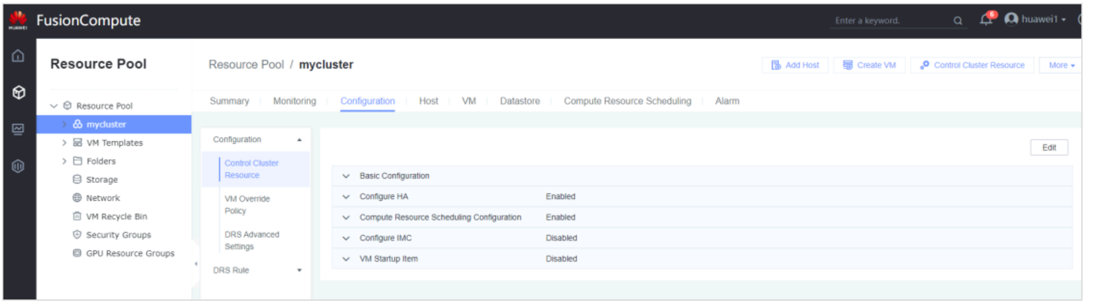
Contents

Cluster management

Function	Description	Navigation Path
Monitoring clusters	Query cluster monitoring information (for example, running status) of a cluster within the specified time period.	**Homepage** > **Resource Pool** > **Cluster**
Configuring cluster attributes	Configure cluster attributes, such as the HA policy, memory overcommitment policy, and VM start policy.	
Configuring resource scheduling policies	Configure the policy for scheduling compute resources in a cluster to implement dynamic resource scheduling and load balancing.	

- FusionCompute resources include host, cluster, network, and storage resources. On FusionCompute, the administrators create clusters or hosts and adjust and schedule host and cluster resources.

Cluster Configuration

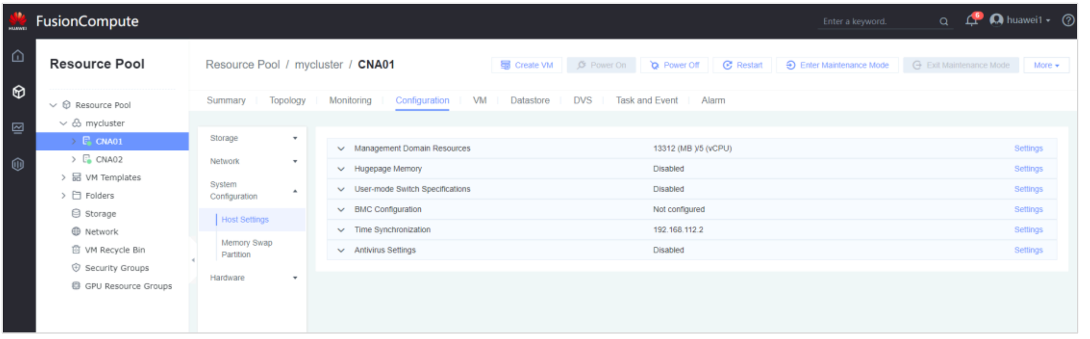


- DRS rules can be configured only after cluster resource scheduling is enabled.

Host Management

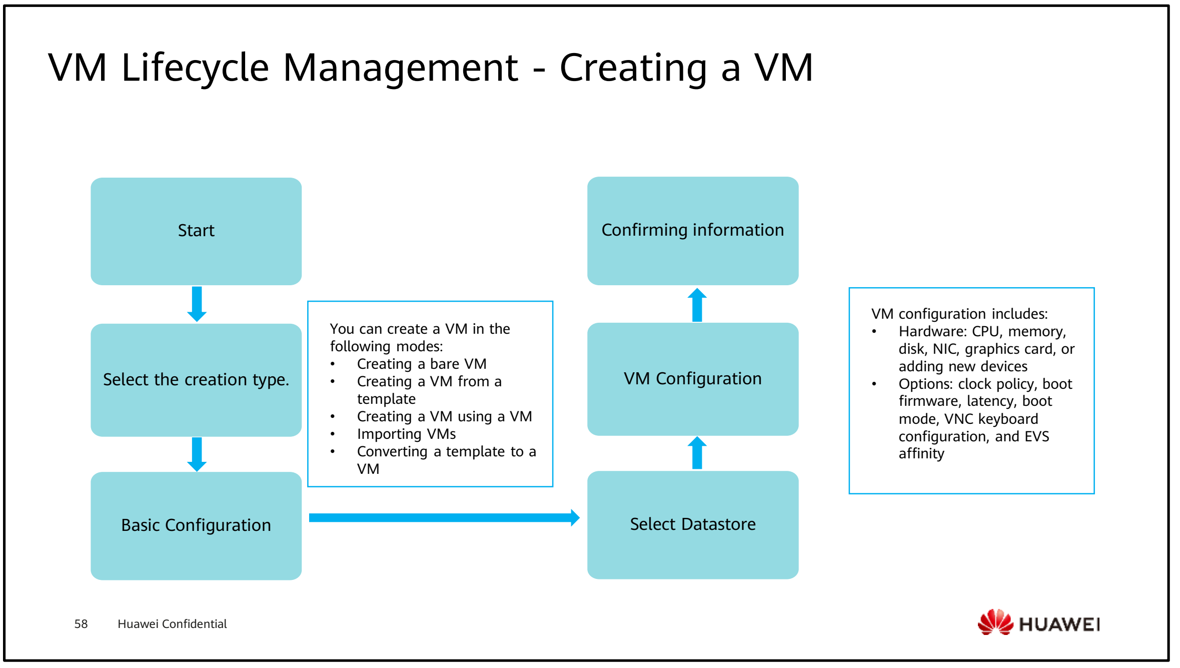
Function	Description	GUI Entry
Monitoring hosts	Query cluster monitoring information (for example, running status) of a cluster within the specified time period.	**Homepage** > **Resource Pool** > **Host**
Configuring host attributes	Configure host attributes, such as time synchronization policy, baseboard management controller (BMC) configuration, multi-path storage type, and maintenance mode.	
Maintaining and managing host ports	Manage and maintain host network ports, such as binding network ports and associating storage ports.	**Homepage** > **Resource Pool** > **Host** > **Configuration**
Associating storage resources with the host	Associate storage resources with the host to provide storage space for the VM on the host.	

Host Management Configuration



- Configure the BMC IP address and BMC username and password for a host. The host can be powered on or off by the system for the purpose of scheduling resources only after BMC parameters have been configured.
- Put a host in maintenance mode. In this mode, the host is isolated from the entire system. This means that maintenance operations, such as parts replacement, power-off, or restart, can be performed on the host without affecting system services. Once a host is in maintenance mode, you must stop or migrate all VMs on the host before actually performing maintenance.
- Configure logical ports of the host to define different network planes.
- Host settings:
  - Host resources
    - Configure the resources reserved for hosts in different scenarios.
  - Hugepage memory configuration
    - Configure the host hugepage memory to optimize memory access efficiency and improve performance.
  - User-mode switch specifications
    - When high network performance is required for a VM, configure the user-mode switching specifications for the host accommodating the VM in advance.
  - BMC configuration
  - Time synchronization
  - Antivirus settings
    - Enable the antivirus function to provide user VMs running on the host with the following services: virus scanning and removal, real-time virus monitoring, network intrusion detection, network vulnerability

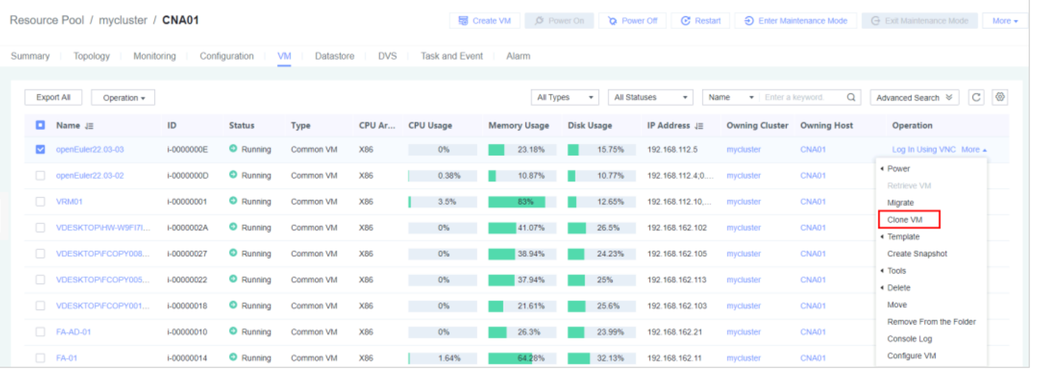
scanning, and firewall.



- Creating a bare VM: A bare VM is a software computer without any OS installed. You can create a VM on a host or in a cluster, and configure VM flavor, such the number of CPUs and NICs, the size of memory or disks.After a bare VM is created, install an OS on it. The procedure for installing an OS on a bare VM is the same as that for installing an OS on a physical computer.
- Creating a VM from a template: Use an existing VM template to create a VM that has similar specifications with the template.
- Converting a template to a VM: All attributes of the VM are the same as those of the template. After the conversion, the template does not exist.
- When VMs are deployed using a template or imported using a template, the VM OS type, OS version, number of disks, capacity, bus type, and number of NICs are inherited from the template. Other attributes can be customized.
- Creating a VM using a VM: Clone a VM to a VM that has similar specifications with the VM.. During VM cloning, the OS type, OS version, number, capacity, bus type, and number of NICs of the VM are inherited from the original VM. Other attributes can be customized.
- Basic configuration includes the VM name and description, VM location, computing resources, whether to bind the VM to the selected host, and OS type and version.

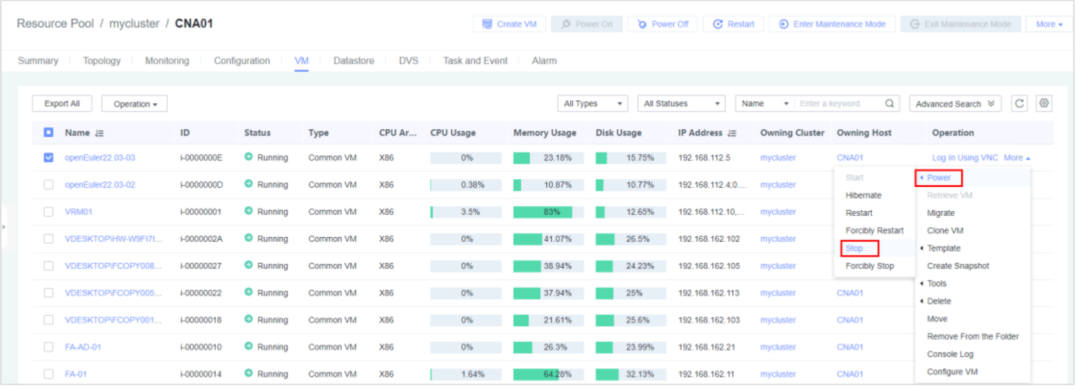
VM Lifecycle Management - Cloning a VM

- Administrators can create VMs by cloning existing VMs on FusionCompute. Some parameters of the clone VM can be modified during creation to make it slightly different from the original one.



HUAWEI

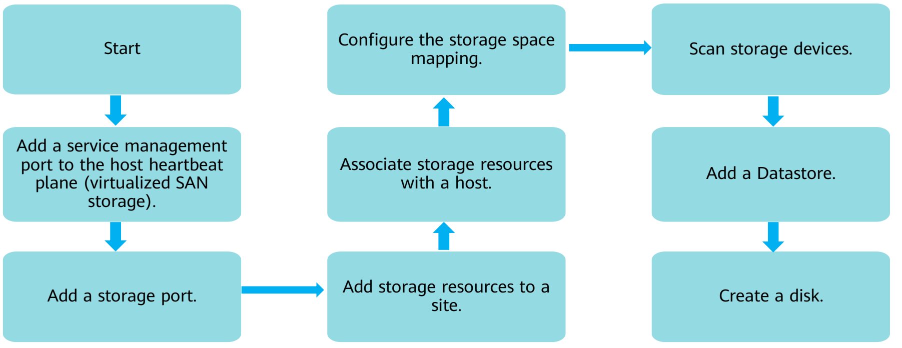
VM Lifecycle Management - Powering Off and Deleting a VM



HUAWEI

Storage Resource Management

- FusionCompute supports storage resources from host local disks or independent storage devices that connect to hosts through network cables or optical fiber cables. Dedicated storage devices are connected to hosts using network cables or fiber cables.



- The process is for reference only and may vary with storage resources or devices. This example is for IP SAN storage.

Network Resource Management

- Network resource management helps guide administrators to create, use, and configure network resources, such as DVSs and port groups.

Network Element (NE)	Description
DVS	A DVS is similar to a switch used for communication on the layer 2 network. A DVS links the port group to the VM and connects to the physical network through the uplink.
Port group	A port group is a virtual logical port similar to a template with network attributes. A port group is used to define VM NIC attributes and uses a DVS to connect to the network. VLAN: Users must manually assign IP addresses to VM NICs. VMs connect to the VLAN defined by the port group.
Uplink	An uplink connects the DVS to the physical network. An uplink is used for VM upstream data transmission.

Contents

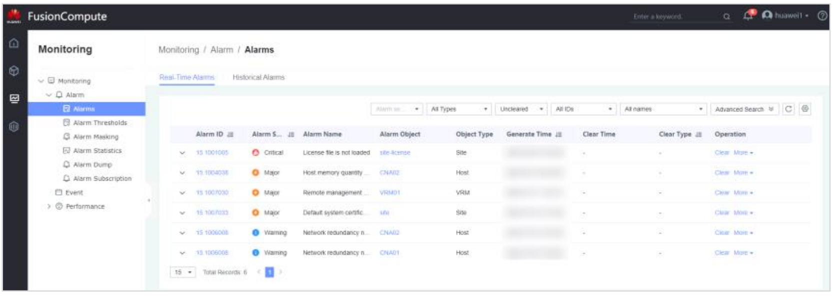
Routine Maintenance Operations

- To ensure long-term and stable running of the system, maintenance engineers need to periodically check the system and rectify the detected faults based on the check results.

Maintenance Item	Check Item	Normal state	Maintenance Interval
Viewing system alarms.	Checking alarms generated on FusionCompute	No new alarm is generated.	Daily
Check the FusionCompute health status.	Health check report	No failed check items are detected.	Daily
Check the device running status.	Indicators on servers, switches, and storage devices	All indicators are normal.	Daily
Check the device running environment.	Temperature and humidity	The ambient humidity and temperature must meet device running requirements.	Weekly
	Air cleanliness	The air quality must meet device running requirements.	Weekly
	Dust proof	Dust accumulation is avoided.	Weekly
heck precaution notices.	Visit https://support.huawei.com/enterprise/en/index.html and choose **Bulletins** > **Warning Notice**s > **Distributed Storage** > **Virtualization** > **FusionCompute**, and check precaution notices.	The requirements described in the precaution notices are met.	Monthly

Alarm management

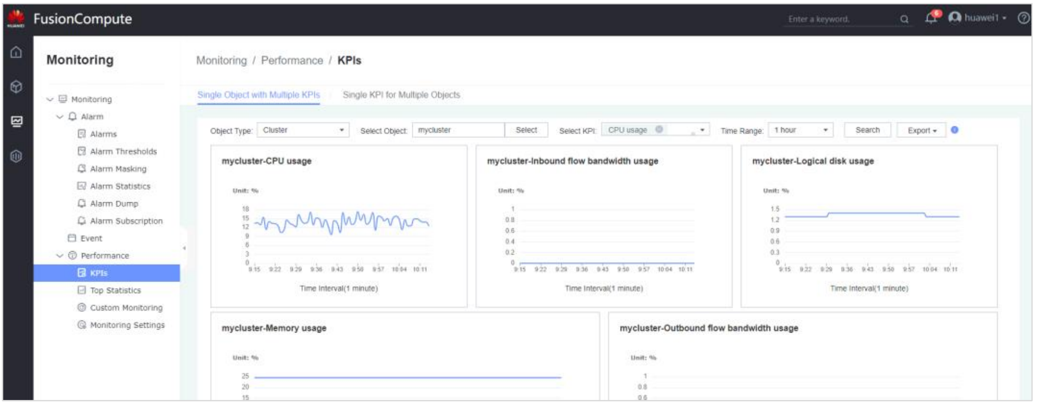
Alarm severity	Icon	Description
Critical		A critical alarm indicates a service-affecting fault and an immediate corrective action is required.
Major		A major alarm indicates a service-affecting fault that needs to be rectified urgently to avoid serious consequences.
Minor		A minor alarm indicates a fault which currently does not affect service and that a corrective action should be taken to prevent a more serious fault.
Warning		A warning alarm indicates a potential or impending service-affecting fault that can be detected before any significant effects have been found.



- FusionCompute alarms severities include critical, major, minor, and warning. After alarms are generated, handle alarms of high severity and then alarms of low severity.

Monitoring management

- Administrators can query cluster, host, and VM information to obtain the cluster running status for a specified period of time.



- FusionCompute can monitor usage of cluster, host, storage, and VM resources. You can choose **Single Object with Multiple KPIs** or **Single KPI for Multiple Objects** to view the resource usage charts.

FusionCompute Account Management

- FusionCompute users include local, domain, and interface interconnection users. A local user can log in to and manage the system. After a domain is created, a domain user can log in to the system. An interface interconnection user supports FusionCompute to interconnect with other components.
- The following table lists the FusionCompute login accounts. (For details about the default passwords, see the related product documentation.)

Login Mode	Default Username/Password	Permission
Common mode	admin/XXXXXX	Has permissions of the system administrator.
Role-based mode	System administrator: sysadmin/XXXXXX Security administrator: secadmin/XXXXXX Security auditor: secauditor/XXXXXX	System administrator: has the permissions to operate and maintain system services and create and delete users. Security administrator: has the permission to manage the rights for users and roles but does not have the permission to create users. Security auditor: has the permission to query and export operation logs of other users.

- When installing FusionCompute, specify the login mode. Once the mode is determined, it cannot be changed.

- By default, the system backs up data at 02:00 each day.
- By default, the system backs up management data at the thirtieth minute of every hour (excluding monitoring data) to the VRM nodes. If no third-party backup server is available, configure one host. The system automatically copies management data to the /opt/backupdb directory on the host. The management data is reserved on the host for only one day.
- By default, the system fetches daily backups on the first day of each month. The system stores a maximum of two backup files, one is collected on the first day of this month, and the other is collected on the first day of the last month.
- If the number of files that are automatically and manually backed up has not reached the upper limit, the new backup files will not overwrite the old backup files. If the number exceeds the upper limit, the system automatically deletes the earliest backup file.
- If a third-party backup server is available and the third-party server backup function is enabled, FusionCompute uploads the backup file stored on the local server to the third-party backup server after an automated or manual backup is complete.
- If the number of files stored on the third-party backup server has not reached the upper limit, the new backup files will not overwrite the old backup files. If the number exceeds the upper limit, the system automatically deletes the earliest backup file.
- During data restoration, do not perform any system operation.

- The system operations include:
  - Creating a cluster
  - Expanding or reducing capacity of a cluster
  - Provisioning services in a cluster
  - Configuring the system management subnet
  - Powering on or off a server
  - Restarting a server

Contents

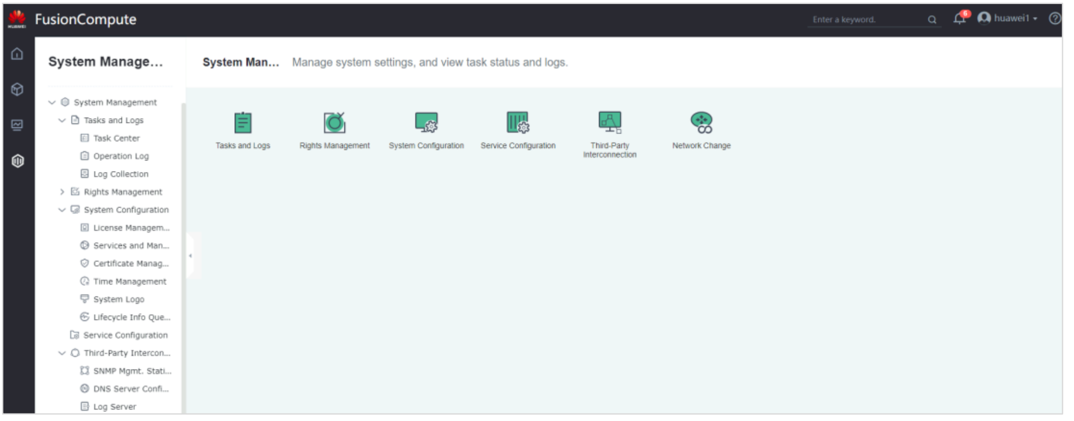
System Configuration(1)

- Administrators can modify FusionCompute configurations as required.
  - Configuring Domain Authentication
  - Updating the License
  - Changing the System Logo
  - Configuring a Login Timeout Period
  - Configuring the Resource Scheduling Interval
  - Configuring an SNMP Station
  - Changing VRM Deployment Mode from Standalone to Active/Standby Mode

  ......

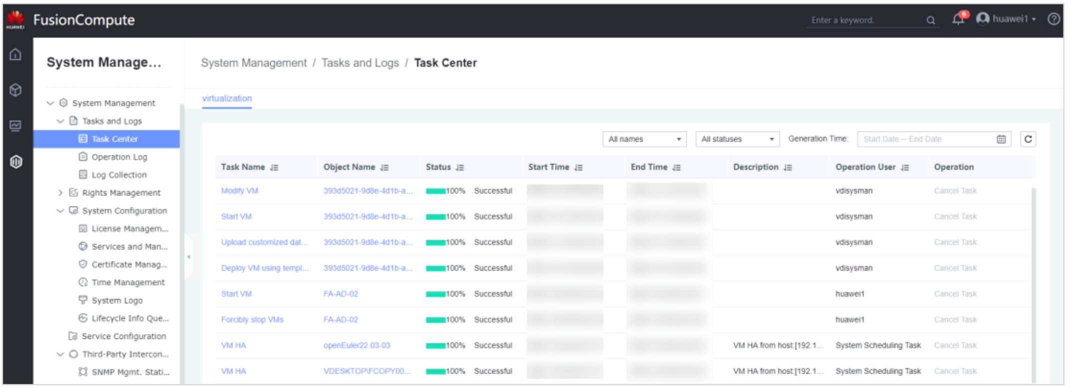
System Configuration(2)

- On FusionCompute, you can view tasks and logs, modify system rights, system configuration, service configuration, and third-party interconnection, and change the network.



Task Management

- Administrators can view the task progress on FusionCompute.



HUAWEI

Quiz

1. (Multiple-Choice) What benefits does the VM migration technology bring to customers?
   A. Automatically recovers services when the VM system is faulty.
   B. Load balancing among physical servers
   C. High reliability of the customer's system
   D. Supports online hardware upgrade.
2. (Multiple-Choice) Which of the following memory overcommitment technologies are available?
   A. Memory sharing
   B. Memory bubble
   C. Memory swapping
   D. Memory Simplified

- Answers:
  - BCD
  - ABC

Summary

- In this chapter, we have learned the computing, storage, and network virtualization features of FusionCompute, and mastered the basic operations of the platform system and resource management. In the following courses, we will continue to learn the development trend of cloud computing technologies.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Abbreviations

- DRS: Storage Dynamic Resource Scheduler
- DVS: Distributed Virtual Switch

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

Overview of FusionAccess

HUAWEI

Foreword

- Huawei FusionAccess is a virtual desktop application based on the Huawei Cloud platform. Software deployed on the cloud platform enables end users to use a thin client or any other device that is connected to the network to access cross-platform applications and their desktops.
- This course describes the architecture and application scenarios of FusionAccess and the principles and functions of HDP.

Objectives

- On completion of this course, you will be able to:
  - Describe the system architecture, benefits, and features of FusionAccess.
  - Learn the functions and principles of HDP.
  - Describe the component architecture and application scenarios of FusionAccess.

Contents

HUAWEI

Traditional PCs: Insufficient Security, Poor Mobility, and Low Maintenance Efficiency

Data Security Threats

- Data is stored on local terminals. Computer faults, virus attacks, and hardware theft may cause data loss, damage, and leakage.
- Various ports and peripherals are difficult to control, and user behavior is difficult to control.

Low efficiency of internal and external collaboration

- Multiple branches and departments of an enterprise cannot collaborate with each other.
- Network disks are used to share data across enterprises, which takes a long time and poses data security risks.

Normalization of hybrid office

- Traditional office forms (host + monitor) are fixed. Mobile office must be equipped with laptops and carried with you, which is a heavy burden.
- Laptop performance is limited, and high-performance office cannot be implemented.

Fixed/Idle office resources

- Traditional office hardware configuration is fixed, and the computing power on the device side is limited.
- Resources cannot be reused during idle hours, and resources are idle during off-peak hours.

Complex O&M management

- There are many software and hardware versions, making it difficult to manage desktops in a standardized manner.
- When a traditional terminal is faulty, IT personnel need to perform onsite maintenance, which takes a long time and affects service continuity.

Cloud-based office, the beginning of the modern office

Driven by technologies and requirements, enterprise office enters the cloud computing era.

PC era

Primary Office Automation

E-mail, Office document electronic, printing, and small-scale instant messaging

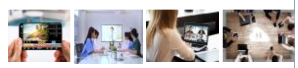
Dot-com era

Internet + Office

Internet-based office applications (Communications, OA applications, online collaboration processes, cloud printing...)

Cloud computing era

Cloud office



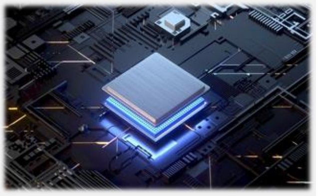
Remote office, video conferencing, cross-PC+mobile office applications, data sharing, cloud storage...

Few terminal types,
limited online applications,
and weak cross-platform collaboration capabilities

Cross-platform, cross-terminal,
cross-time and place processes can be continuous,
data can be synchronized, and resources can be shared.

Requirements: Future Challenges Accelerate Government and Enterprise Office Transformation

Faster Transformation



- Cloud-based office transformation, and popularization of office applications.
- Office application adaptation, migration, and reconstruction using proprietary CPU chips and Oss.

Broader Collaboration

- More real-time teamwork: instant messaging, online document storage, online meetings, and file sharing.
- Expanding collaboration scope: file access management, document editing, and task management.

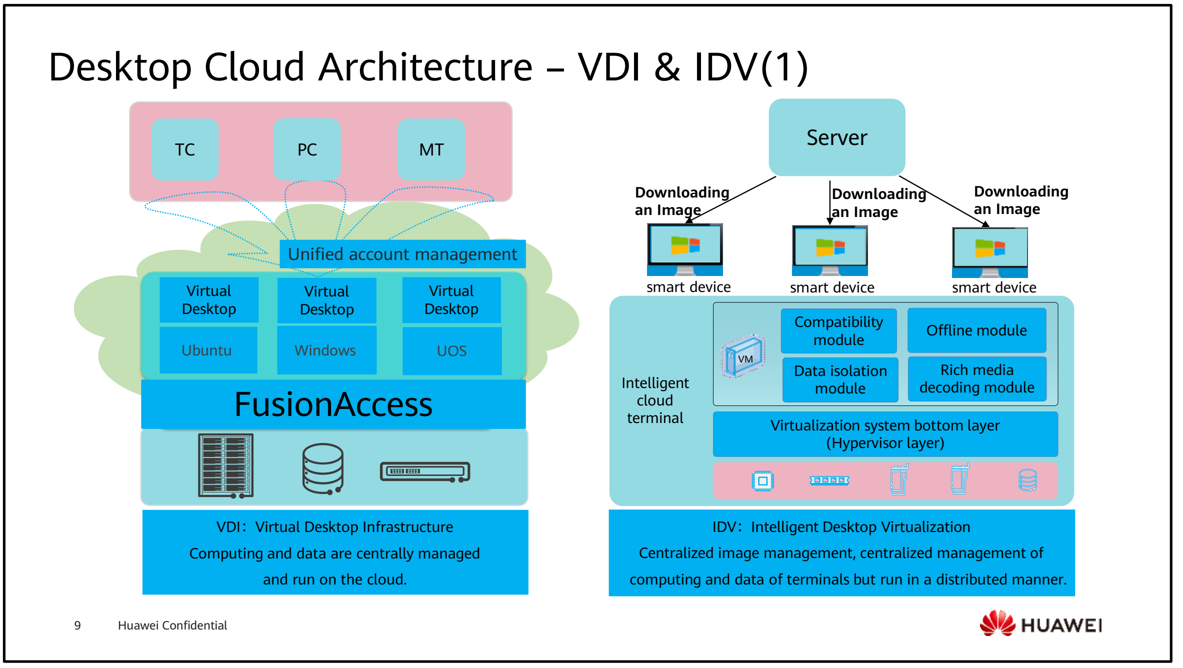
Greater Security Threats

- Identity authentication and access permission management are harder for mobile offices.
- Transmission and storage of important/ sensitive office data must be secure to prevent data leak and threats.

Cloud-based office, the beginning of the modern office

What Is Desktop Cloud?

- Desktop cloud is a mature cloud computing application, which centralizes computing and storage resources from terminals (PCs) to data centers for virtualization and centralized management. Users can use cloud terminals (Thin Client, Software Client and Android/iOS mobile terminal) to access the personal desktop space on the network. It enables users to access and use data and applications in the data center through any terminal and any network.
- FusionAccess is a virtual desktop application deployed on hardware that enables end users to access cross-platform applications and virtual desktops using thin clients (TCs) or other networked devices.



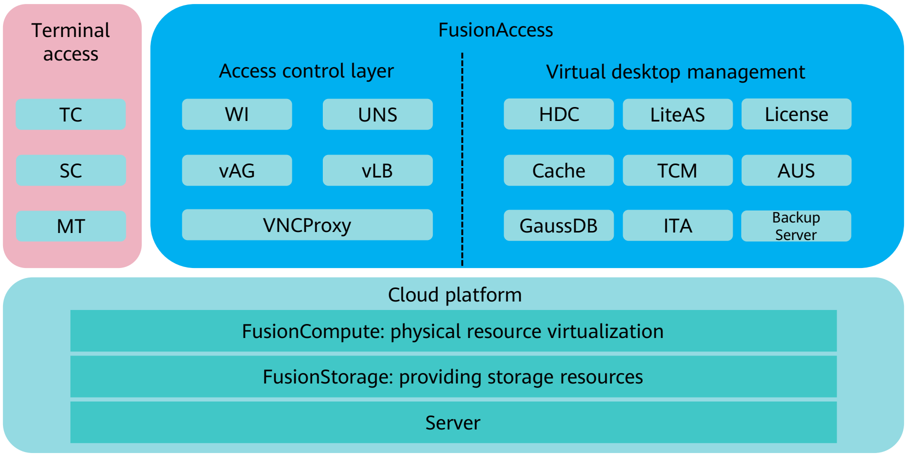
- Technology Comparison
  - An IDV represents a small step forward from a traditional PC-based office architecture. Typically, it consists of an image server, management software, and local virtual desktop terminals (fat clients). A VDI, in contrast, is a completely new design. Instead of PCs, it uses TCs and cloud virtual desktops, which can be scaled out using any kind of terminals you want, as no data is stored locally. With a VDI, the security, O&M, and low resource utilization pain points of a traditional PC-based office are all addressed.
  - The IDV solution uses local virtual desktops, which means there is a more complex mix of terminals in use and management and maintenance are more difficult. When a large number of terminals need to be managed, a complex server is required to centrally manage terminal images and synchronize data distributed on terminals.
  - In certain scenarios, IDV can work offline, but the number of applications that can run offline has been decreasing. As investment into network infrastructure continues, we will eventually see offline applications become a thing of the past.
- Industry Trends
  - VDI is favored by mainstream vendors such as Huawei, Citrix, and VMware (data of IDC: top 3 vendors in China in terms of the virtual desktop market share), while IDV is used only by some Chinese vendors such as Ruijie and OS-Easy.
  - VDI's integration with cloud makes it future proof.

Desktop Cloud Architecture – VDI & IDV(2)

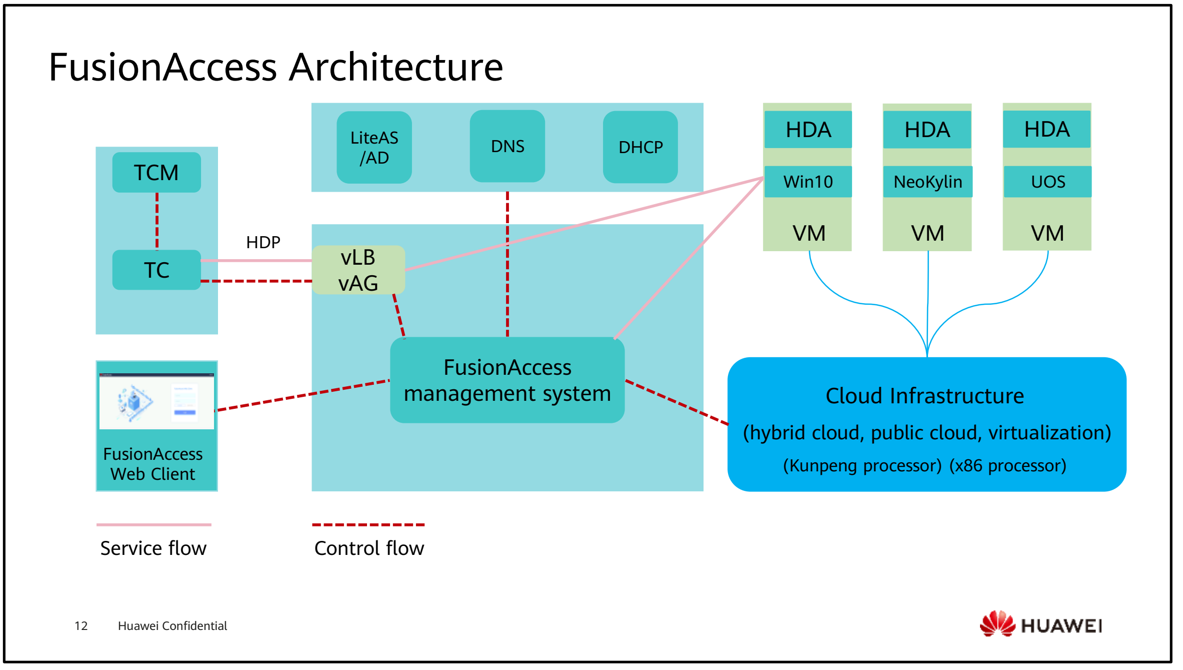
Item	VDI	IDV	Remarks
Data Security	High. Centralized data storage prevents data leakage through terminal access.	Low. Data is downloaded to the terminals, which makes data leakage more likely.	Centralized data storage is more secure than local storage.
Terminal Maintenance	Easy. Terminals only provide access. No maintenance is required. Faulty terminals can be replaced at any time.	Difficult. Terminals provide services. Complex maintenance is unavoidable.	In a centralized architecture, terminal faults can only be rectified manually.
System Reliability	High. Cloud-based resources support time-based scheduling and dynamic allocation. Hardware faults can be fixed automatically.	Low. Manual intervention is required when a terminal fault occurs.	If IDV data is not synchronized to the server in a timely manner, data may be lost or inconsistent.
Terminal Requirements	None	The CPU must support virtualization and dual-OS installation. TCs are not supported.	CPUs that support virtualization are expensive and waste power.
Mobile Terminals	Support	No	With IDV, only certain terminals are supported.
Mobile Office	Support	No	In an IDV solution, if a terminal is replaced, the image needs to be pulled again.

- The hardware requirements are divided into two parts. The preceding table lists only the requirements of terminal hardware. The hardware configuration of the server is as follows:
  - VDI desktop virtualization adopts the data centralization design. Therefore, servers that manage virtual desktops must have high hardware configurations, including CPU, memory, and hard disks. Therefore, more virtual desktop users need to use the virtual desktops. Therefore, high initial construction investment is required.
  - IDV desktop virtualization makes full use of hardware resources of cloud terminals for data storage and computing. It has high requirements on hardware of cloud terminals but does not have strong requirements on server configuration, which facilitates reuse.
- Indicates whether to support offline office. The options are as follows:
  - All computing in VDI desktop virtualization is implemented on the server. If the server is faulty or disconnected from the network, cloud terminals cannot invoke resources on the server and cannot work properly.
  - IDV desktop virtualization is different. It invokes cloud terminals and resources for storage and computing. When a server is faulty, terminals can still work offline.

FusionAccess General Logical Architecture

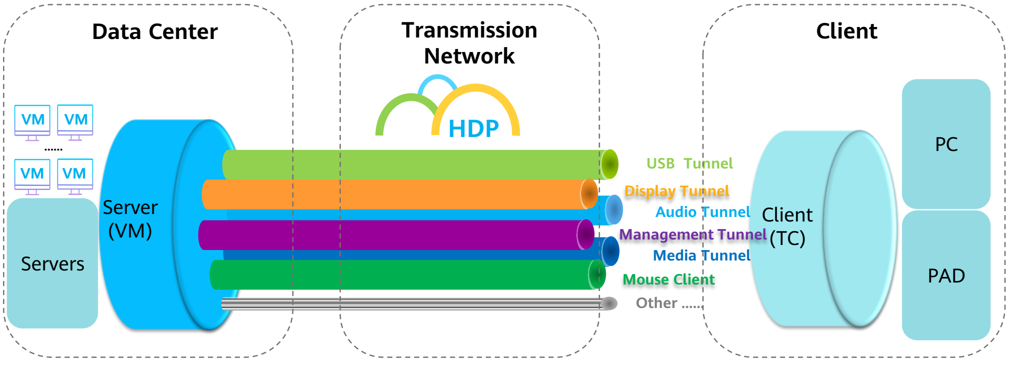


- The logical architecture of the FusionAccess solution consists of FusionAccess, FusionCompute, and FusionStorage.
  - FusionAccess is the desktop management software that consists of the access control layer and virtual desktop management layer. It provides a graphical user interface (GUI) portal for administrators of carriers or enterprises to quickly provision, maintain, and reclaim virtual desktops, improving resource utilization and reducing the operational expenditure (OPEX).
  - FusionCompute is the cloud OS software that virtualizes compute, storage, and network resources, and manages virtualization, service, and user resources in a centralized manner. It also centrally allocates and manages these virtual resources using unified interfaces, ensuring system security and reliability while reducing the OPEX. FusionCompute helps carriers and enterprises build secure, green, and energy-saving cloud data centers.
  - FusionStorage is a storage product that uses storage system software to build a fully distributed storage pool of local storage resources and provide block storage services for upper-layer applications.



- Huawei FusionAccess desktop cloud solution was launched in 2009. After more than 10 years of careful polishing and market verification, Huawei FusionAccess desktop cloud solution has ranked No. 1 in China's desktop cloud market share for seven consecutive years.
- In December 2019, Huawei launched FusionAccess 8.0, the industry's first desktop cloud solution based on Kunpeng processors, achieving end-to-end independent innovation in full-stack software and hardware.
  - Ecosystem Cooperation: Huawei has reached cooperation with mainstream software vendors in China, and has been compatible with mainstream Chinese operating systems such as UOS and Kirin, 470+ application software, and 1000+ peripherals, fully meeting the requirements of domestic replacement in OA scenarios.
  - Performance: Huawei Kunpeng desktop cloud provides ultimate experience comparable to mainstream x86 PCs. In addition, Huawei FusionAccess supports the dual-stack architecture of "x86+Chinese-made chips" and unified management of Windows desktops and Chinese desktops.

Technical Principles of FusionAccess

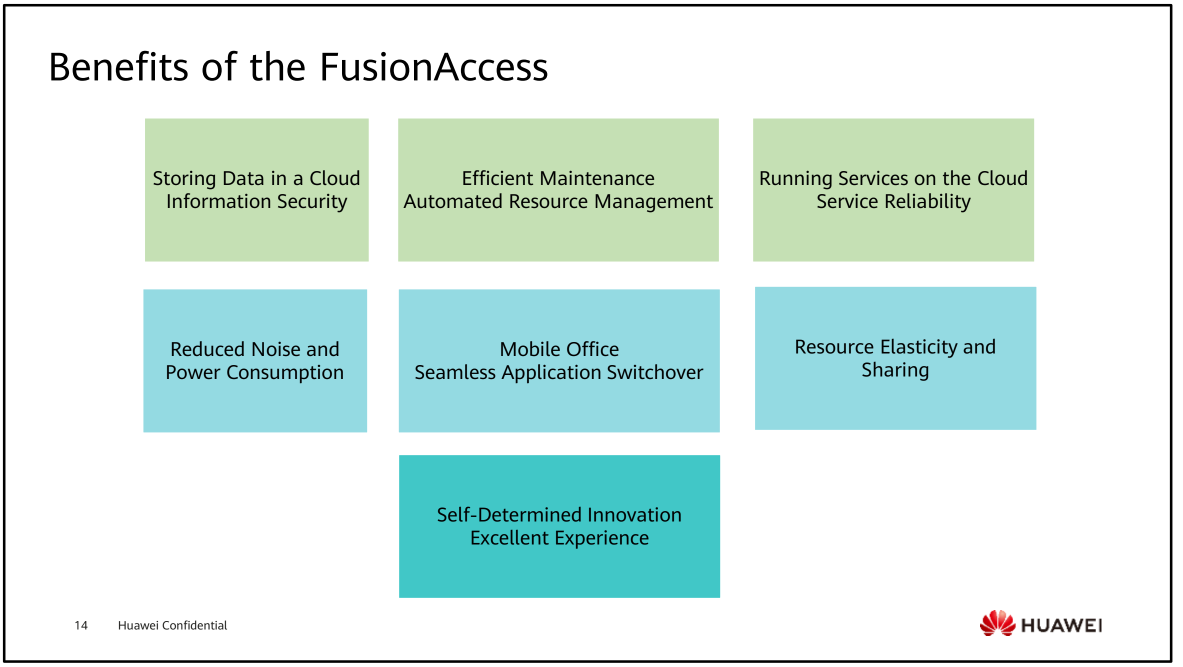


The interaction between the client and server:

1.Service load and computing are performed on VMs in the data center. Images are projected frame by frame to terminals through the HDP protocol. After being decoded, the terminals display the images on monitors to interact with users.

2.The HDP protocol does not transmit specific service data. Service data is always running in the data center, ensuring data security.

HUAWEI



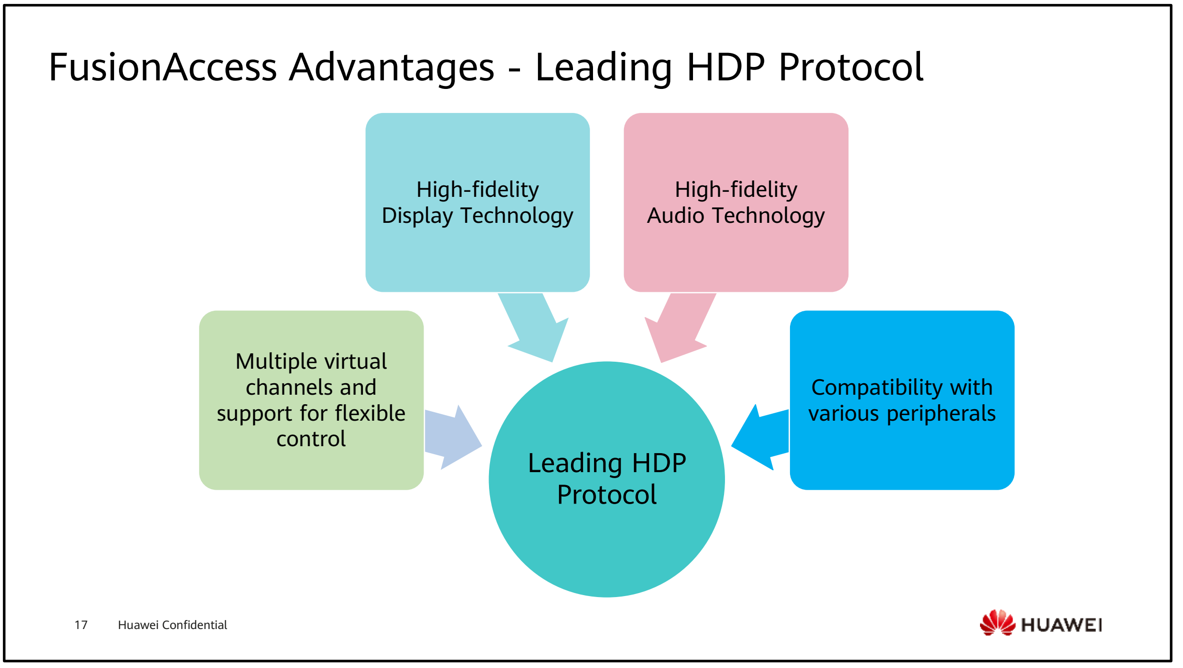
- Information Security Protected by Storing Data in a Cloud: In conventional PC desktop environments, user data is stored in local PCs. Data breach or loss may occur due to cyber attacks. However, in desktop cloud environments, data is stored and processed on servers rather than user terminals, preventing data breach or loss. In addition, security mechanisms such as TC access authentication and encrypted data transfer are employed to ensure the security and reliability of the desktop cloud system.
- Automated Resource Management and Efficient Maintenance: Conventional PC desktop systems suffer a high failure rate. According to statistics, an IT professional is required on average for managing and maintaining 400 PCs, and the maintenance procedure for each PC requires 2 to 4 hours. The FusionAccess desktop solution has the following advantages:
  - Improved maintenance efficiency: FusionAccess provides a powerful one-click self-service maintenance tool that enables enterprise employees to maintain their virtual desktops by themselves. In addition, it also allows one IT professional to centrally manage and maintain more than 2000 virtual desktops, improving the maintenance efficiency by 4-folds.
  - Automated resource management: In the daytime, resource usage is automatically monitored to ensure load balancing among servers. At night, physical machines not in use are shut down to save energy.

- Service Reliability Ensured by Running Services on the Cloud: In conventional PC desktop environments, all services and applications run on local PCs, with a 99.5% availability and annual downtime of 21 hours. However, with FusionAccess, all applications and services run in cloud data centers, which delivers 99.9% availability. The reliable and smooth running of applications greatly reduces management and maintenance costs of office environments.
- Mobile Office Enabled by Seamless Application Switchover: Traditionally, users can only access their desktops from a dedicated device. However, with FusionAccess, users, either in offices or on a trip, can access their desktops at any time, from anywhere. In addition, users can move from one place to another during work without interrupting applications, because data and desktops are running and stored in cloud data centers.
- Reduced Noise and Power Consumption: Energy-efficient TCs minimize noises and lower the temperature in offices. After TCs are deployed, noises in offices are reduced from 50 dB to 10 dB. The total power consumption of a TC and liquid crystal display (LCD) is about 60 W. This means a 70% decrease in electricity bills compared with a conventional PC. Reduced power consumption also decreases temperature control costs.
- Resource Elasticity and Sharing
    - On-demand resource allocation: FusionAccess centrally manages and

  allocates resources on demand because all resources are stored in cloud data centers.
  - Improved resource utilization: Centralized resource sharing improves resource utilization considerably. The CPU usage of conventional PCs ranges from 5% to 20%, while that of cloud data centers of FusionAccess can reach about 60%, greatly higher than the former.
- Excellent Experience Brought by Self-Determined Innovation: FusionAccess is the first Kunpeng-powered end-to-end desktop cloud product that uses Huawei's in-house software and hardware in the industry and is compatible with China-developed desktop OSs and ecosystems. The in-house Huawei Desktop Protocol (HDP) provides the best display, audio, and video quality. The distributed all-flash storage offers high performance and low latency, handling large numbers of concurrent I/O requests easily and delivering fast desktop experience.

FusionAccess Advantages

- Leading HDP Protocol
- Flexible Desktop Deployment
- E2E Security Design
- E2E Solution
- Proprietary Cloud Software
- High-Reliability Solution
- Large-scale Delivery and Implementation
- Brand Services



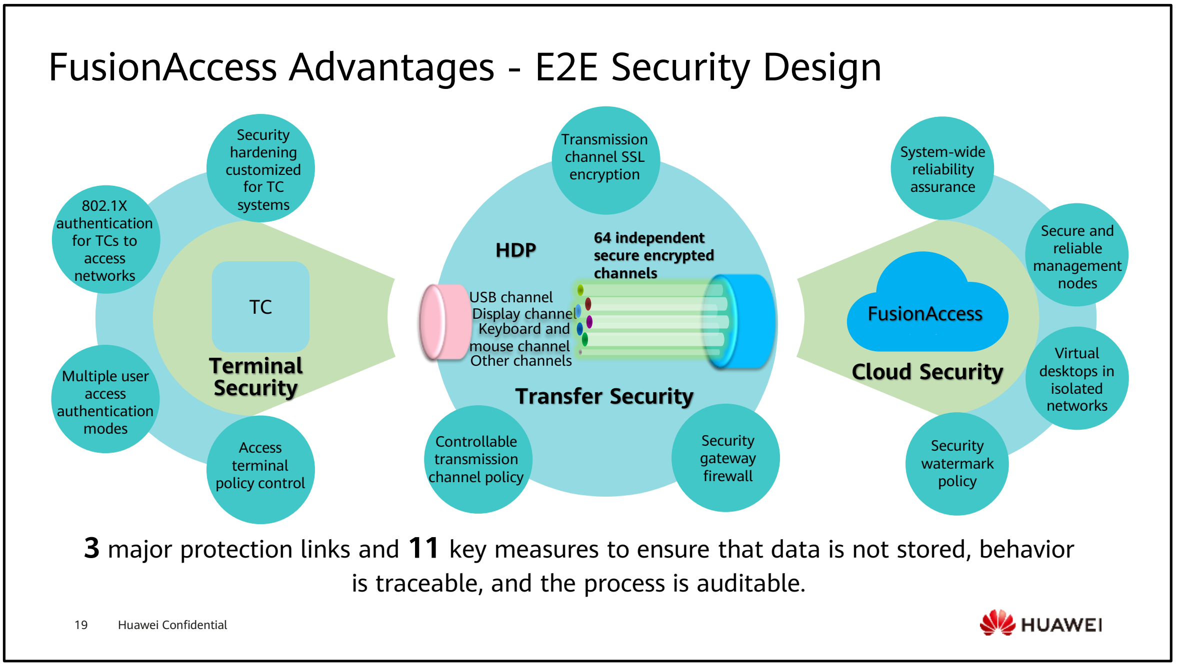
- Multiple virtual channels and support for flexible control: HDP supports a maximum of 64 virtual channels. Each virtual channel bears different upper-layer application protocols. The virtual channels ensure communication security and good user experience based on quality of service (QoS) priorities (for example, the keyboard and mouse virtual channel can be given the top priority).
- High-fidelity Display Technology: HDP adopts lossless compression algorithm for texts and lossy compression algorithm for natural images to achieve a balance between bandwidth and display effect. HDP automatically detects unchanged images and transmits changed image data only to save bandwidth. The UDP-based self-developed Intelligent Display Transport (IDT) protocol is provided to reduce the requirements for network bandwidth, delay, and packet loss rate. HDP also enhances the QoS tolerance of the desktop office network, intelligently detects network quality, and automatically adjusts application layer policies to reduce traffic transmission and congestion.
- High-fidelity Audio Technology： Automatically identifies video playback scenarios, uses efficient algorithms for encoding, dynamically adjusts the video frame rate based on the network quality, preferentially ensures video smoothness, and makes full use of TC hardware capabilities for decoding. Huawei-developed video accelerator, which makes full use of the hardware decoding capability of TCs, supports automatic reconnection and playback upon disconnection, dynamic traffic adjustment, and supports up to 4K video playback. The smoothness is better than that of similar products.
- Compatibility with various peripherals: HDP supports various peripherals, including USB devices and printers. HDP can be quickly customized to be

compatible with customers' peripherals.

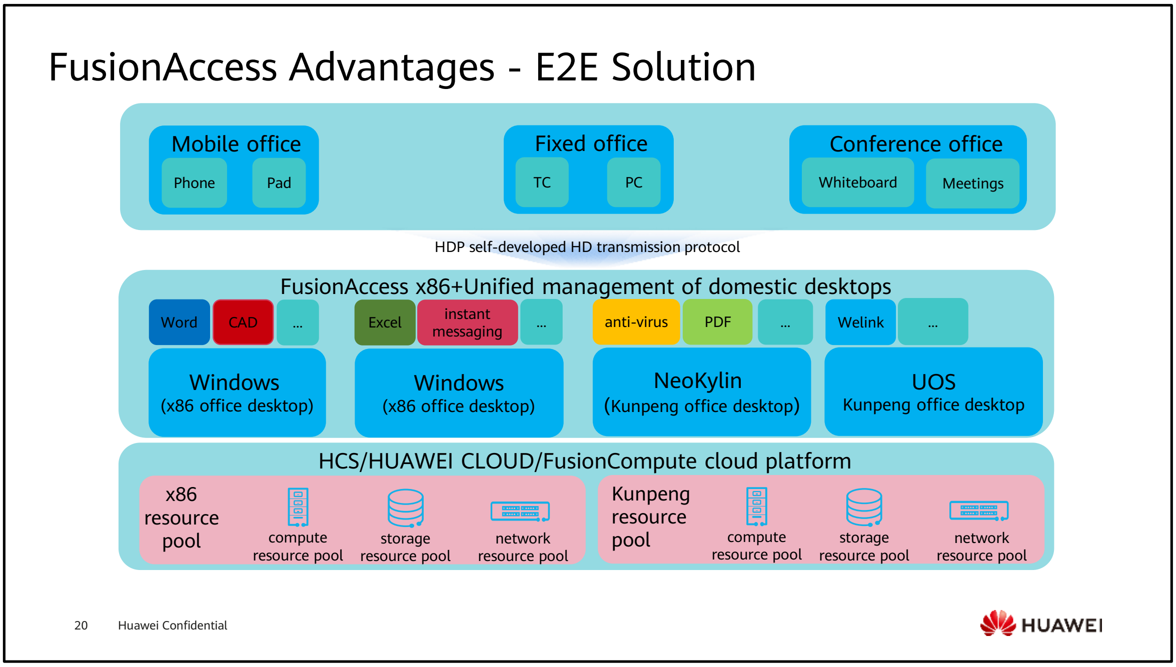
FusionAccess Advantages - Flexible Desktop Deployment

Scenario Category	Scenario Description	Deployment Model
Personalized program and data	●Users have personalized application installation requirements. ●Users have personal data storage requirements. ●Typical scenarios: daily office、R&D office	● 1:1 private desktop (full copy desktop)
No personalized program but personalized data	●Users do not have personalized application installation requirements. ●Users have personal data storage requirements. ●Typical scenario: call center	● M:N pooled desktops (linked clone desktops) ● Personal data and configuration: NAS web disks and profile roaming are used to store personal data.
No personalized program and data	●Users do not have personalized application installation requirements. ●Users do not need to store personal data. ●Typical scenarios: meeting rooms、training classrooms	● M:N pooled desktops (linked clone desktops) + automatic restoration upon shutdown

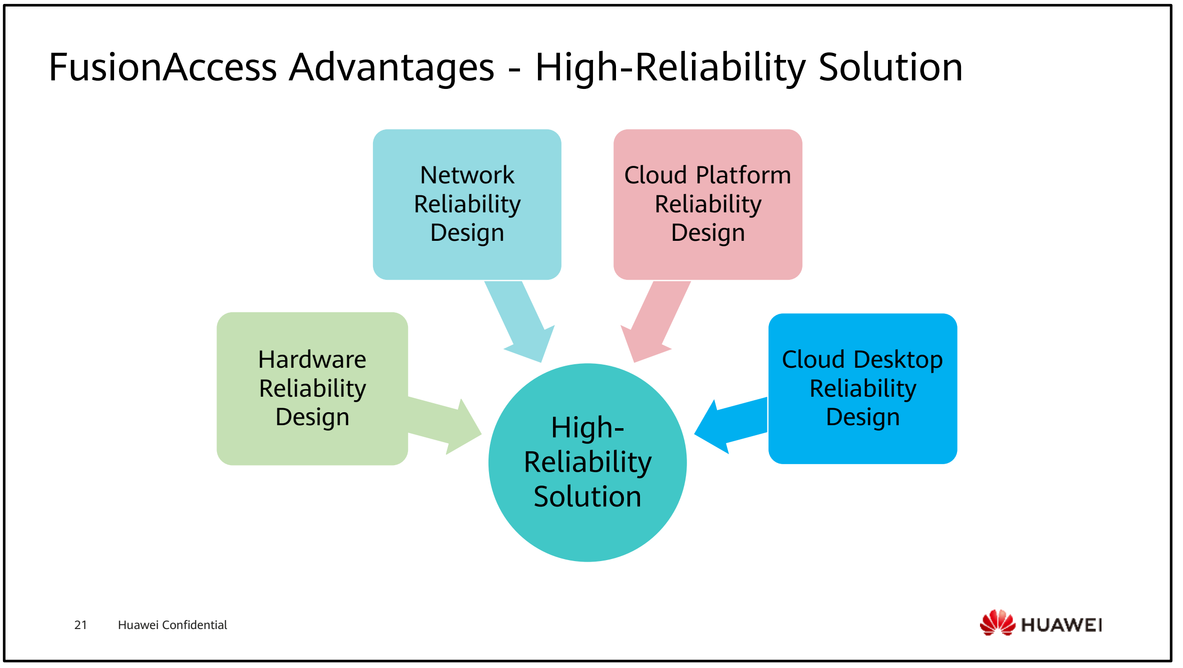
- 1:1 dedicated desktops are recommended for scenarios where personalized applications and data are required, such as common OA and R&D offices. A virtual desktop is created in full copy mode. The system allocates an independent system disk space and data disk space to the virtual desktop, and copies the VM template to the system disk. In this way, each virtual desktop has an independent system disk and user data disk. VM-level isolation features high security and customization. Various types of peripherals are supported. User experience is the same as that of traditional PCs. VM specifications can be flexibly adjusted based on user workloads.
- M:N pooled desktops are recommended for non-personalized application scenarios, such as conference rooms and training classrooms. Linked clone is used when virtual desktops are created. The system automatically creates a shared system base volume. All user VMs use this system base volume. The system creates a delta volume for each VM to temporarily store user data changes. When the desktop is shut down and restarts, The differential data disk is restored to implement power-off restoration. For users who have personalized data storage requirements, a NAS network disk can be allocated to each user to store personalized data and configurations. The personalized configuration is implemented through profile roaming of the AD domain policy. In this way, users can have the same desktop experience and user data when logging in to each desktop.



- To ensure security of data centers, the cloud computing system adopts a complete security architecture to enhance network isolation and virtualization isolation. This security architecture follows the ideas of layered defense and in-depth defense.
- The Huawei FusionAccess desktop system implements access control, security control, rights control, operation audit, and data protection to prevent unauthorized access to the data center, loss of data, and denial of illegal activities.



- Huawei constantly enhances its innovation capability and core competitiveness by expanding its footprints and building delivery centers all over the world, including Shenzhen, Xi'an, Beijing, Hangzhou, and Chengdu.
- Huawei provides E2E products covering terminals, servers, storage devices, network devices, security devices, virtualization software, and desktop cloud software in FusionAccess desktop solution to ensure good user experience and compatibility.

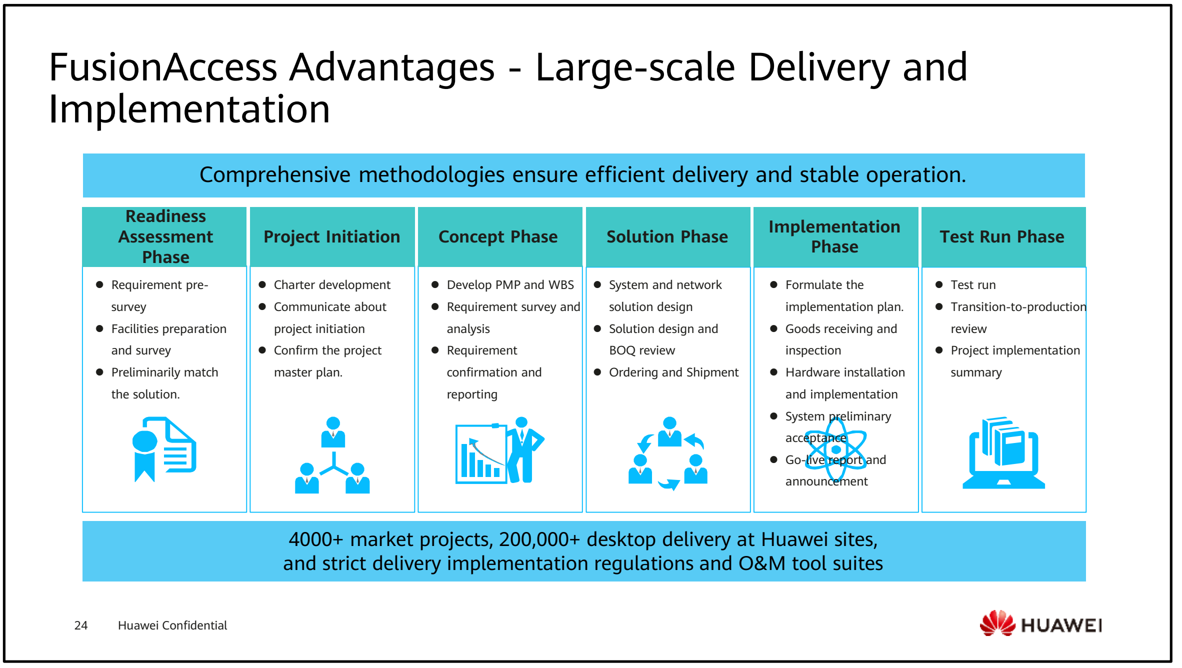


- The desktop cloud platform directly carries users' cloud office services, which are dense and light office services. Compared with the traditional distributed deployment of PCs, the desktop cloud platform has higher reliability requirements. Huawei desktop cloud solution is designed based on the reliability of the hardware platform, network plane, cloud platform, and cloud desktop.
- Hardware Reliability Design:
    - Reliability of equipment rooms, cabinets, wind, fire, water, and other infrastructures
    - Servers support component redundancy design and intelligent fault detection mechanisms.
    - The storage system supports multiple copies and EC.
- Network Reliability Design:
    - The network communicates with each other on different planes. The management, service, and storage planes are planned to ensure that traffic does not interfere with each other.
    - Switches are stacked in redundancy mode, improving reliability and reducing O&M costs.
    - Network adapters are bound to work in redundancy mode to improve load sharing and link reliability.

- Cloud Desktop Reliability Design:
  - The desktop cloud client supports automatic reconnection of desktop sessions, ensuring user experience when the network is unstable.
  - The desktop cloud port supports the anti-collision mechanism, ensuring that desktops can be used normally even when port conflicts occur.
  - The desktop cloud agent supports a high-reliability mechanism. Even if the desktop cloud agent is interrupted unexpectedly, the desktop cloud agent can automatically start and recover.
  - The desktop cloud supports the self-service maintenance console to ensure that emergency channels can be used to rectify VM network faults.

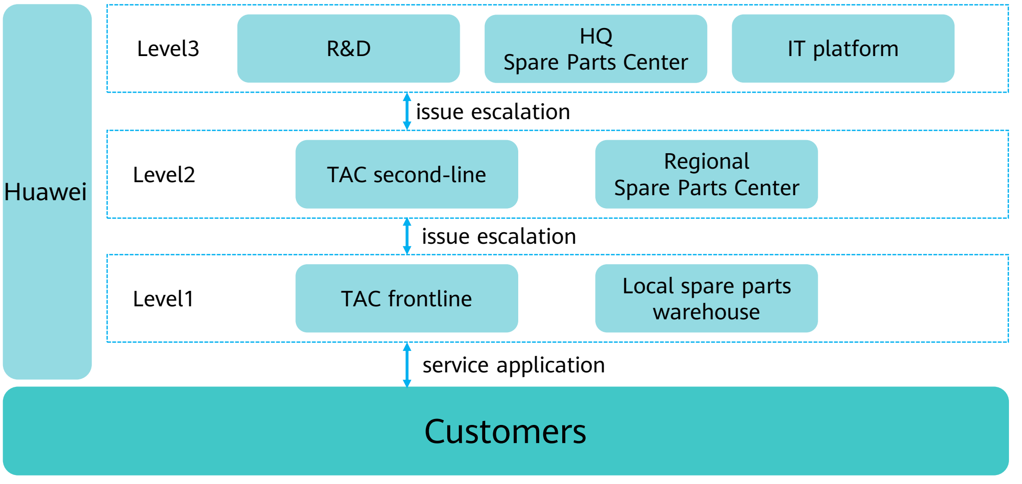
FusionAccess Advantages - Proprietary Cloud Software

- To ensure information security, solutions that have intellectual property rights are required, especially in security scenarios.
- Based on the mature FusionSphere, Huawei-developed and proprietary controllable FusionAccess has passed tests of China Information Security Evaluation Center, Ministry of Public Security, and People's Liberation Army, and provides multi-level protection in aspects of terminal access, access security, management security, and user data security.



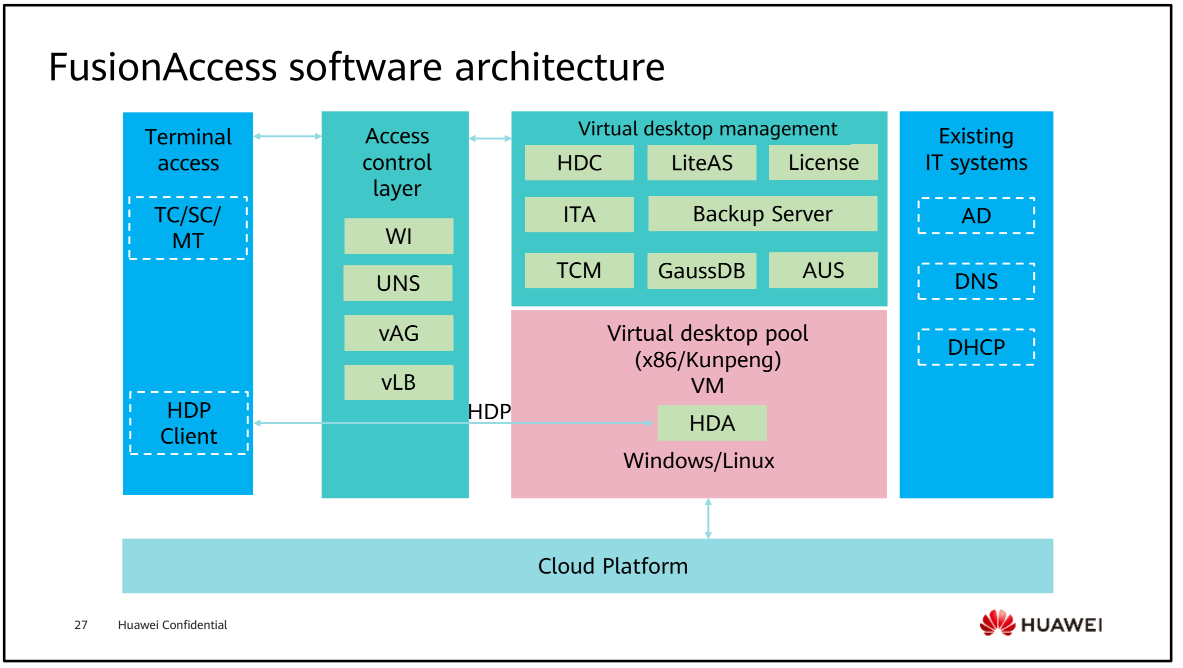
- Huawei has deployed the world's largest desktop (serving more than 200,000 users) and accumulated extensive delivery and O&M experience. The whole solution, includes the cloud software, servers, storage devices, switches, and terminals, has been verified in commercial use.
- At the same time, Huawei has put the FusionAccess desktop solution into commercial use for 4800 customers in more than 110 countries and regions, and made breakthroughs in major industries, for example, Agricultural Bank of China, Sinopec, State Grid, Huazhong University of Science and Technology, Shenzhen Stock Exchange, CCTV, Saudi Arabia TVTC and so on.

FusionAccess Advantages - Brand Services



- The services of Huawei cloud computing products are delivered by Huawei. With its professional local delivery and sales support team, any post-sales problems can be fast solved and customers' specific requirements can be fulfilled. This prevents shifting responsibilities between manufacturers or slow response of problem handling due to too many components involved or difficult problem locating.

Contents



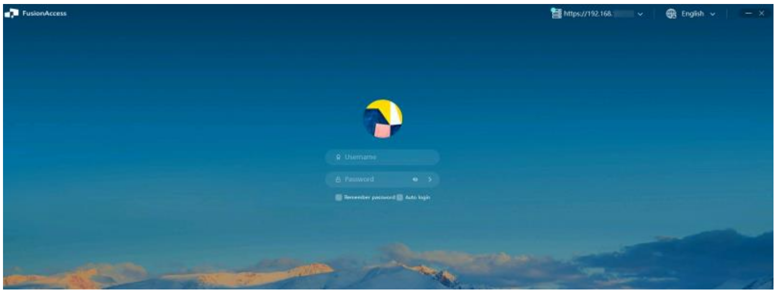
- HDP Client: Installed on terminals that are used to access virtual desktops.
- Huawei Desktop Agent (HDA): Installed on computers and enables computers to interact with desktop management components and access terminals.
- FusionCompute and the cloud platform reside on the management plane. FusionAccess and its components reside on the service plane. TCs, SCs, and mobile terminals reside on the user plane.

Cloud terminal

- Cloud terminals provide desktop display, keyboard, and mouse functions. The TC/SC accesses a specified virtual desktop through an access gateway. The HDP protocol encrypted by using the Secure Sockets Layer (SSL) protocol is used to transmit data between the TC/SC and the access gateway. Users can configure policies to enable or disable the redirection from peripherals, such as USB devices, to virtual desktops. With TCs/SCs, users can access virtual desktops by using domain accounts.
- When users are outside of their offices, they can achieve mobile office by accessing their virtual desktops using HUAWEI MediaPad M6 or laptops through 4G, 5G, or Wi-Fi connections.

Access Control Layer(1)

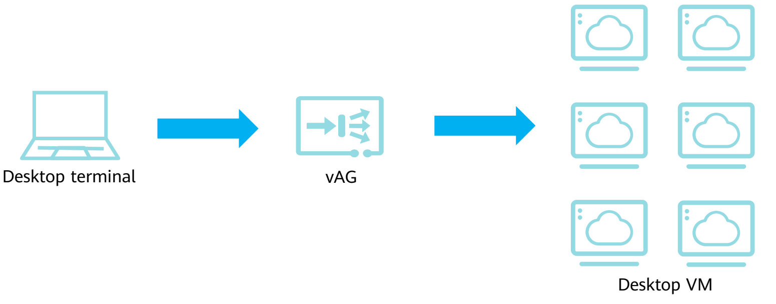
- WI: Web Interface
  - The WI provides a web login page for users. After a user initiates a login request, the WI forwards the user login information (the encrypted username and password) to the LiteAS for authentication. If the authentication succeeds, the WI displays a computer list provided by the HDC to the user. The user can choose a computer from the list to log in to.



- Users can connect to, start, and restart VMs on the WI.

Access Control Layer(2)

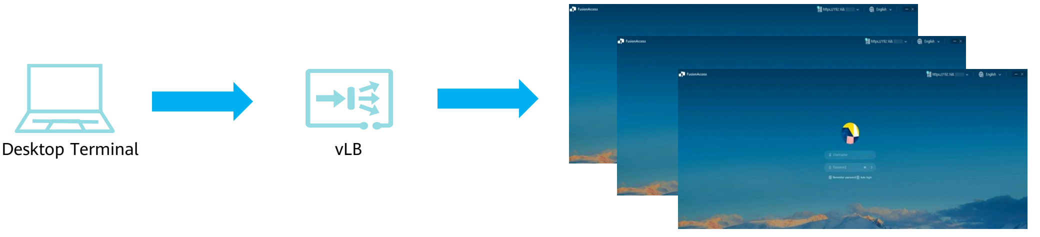
- vAG: Virtual Access Gateway
  - The vAG is used as desktop access gateway and self-service console gateway. When a user computer is faulty, a user cannot log in to it using a desktop protocol. In this case, the user can use the VNC self-service console to log in to the faulty computer and perform self-service maintenance.



- In FusionCompute 8.2.0 or later, the function of the VNC self-maintenance console is implemented by the VNCProxy component.
- The access gateway component connects the user terminal access network and the desktop service network. It provides the access gateway and HDP over SSL encryption functions for clients and virtual desktops to improve system security.
- Load balancer and access gateway support hardware and software.

Access Control Layer(3)

- vLB: Virtual Load Balance
  - The LB implements load balancing between WIs to prevent a large number of users from accessing the same WI. This can be implemented by deploying the vLB.
  - The vLB can automatically perform health check on the WI to ensure that all requests are allocated to working WIs.



- The vLB implements load balancing between WIs as follows: The IP addresses of multiple WIs are bound to one domain name. When users enter the domain name to send login requests, the vLB resolves the domain name to WI IP addresses according to the IP address binding sequence, and evenly allocates the users' login requests to the WIs whose IP addresses are resolved. In this way, the vLB ensures the reliability of the WIs and accelerates WI response.

Access Control Layer(4)

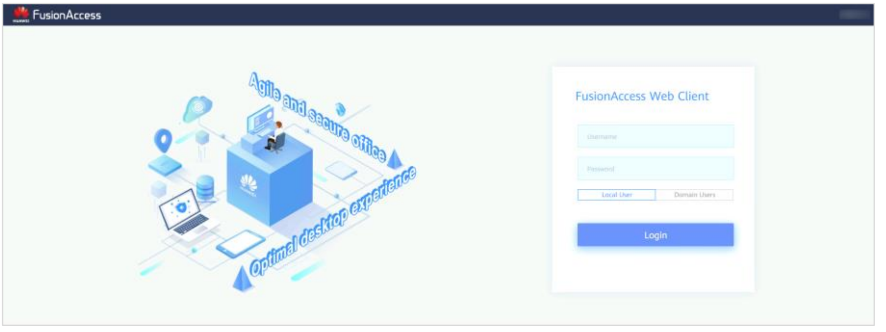
- UNS: Unified Name Service
  - The UNS allows users to access multiple FusionAccess systems with different WI domain names using a unified domain name or IP address, removing the need to switch between WI domain names.

Access Control Layer(5)

- VNCProxy: Self-help console
  - When a user computer is faulty, a user cannot log in to it using a desktop protocol. In this case, the user can use the VNC self-service console to log in to the faulty computer and perform self-service maintenance.

Virtual Desktop Management Layer(1)

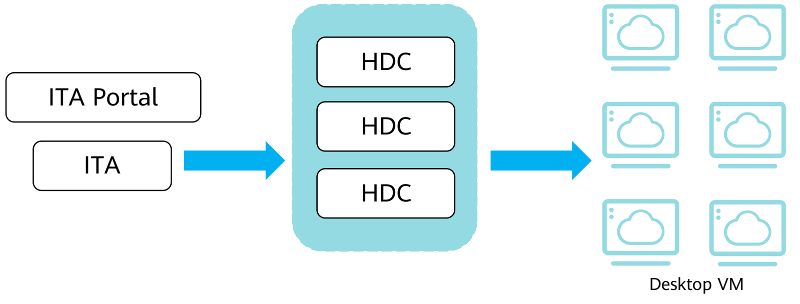
- ITA: IT Adaptor
    - The ITA provides interfaces for users to manage computers. It interacts with the HDC and the FusionCompute cloud platform software to create and assign computers, manage computer statuses and templates, and operate and maintain computers.



- VM creation, provisioning, and routine maintenance are performed on the ITA portal. The ITA invokes the interfaces provided by the HDC.
- The ITA is a web service based on Tomcat. It provides unified interfaces for the IT portal and integrates interfaces for the HDC, FusionCompute, VMs, and DNS.

Virtual Desktop Management Layer(2)

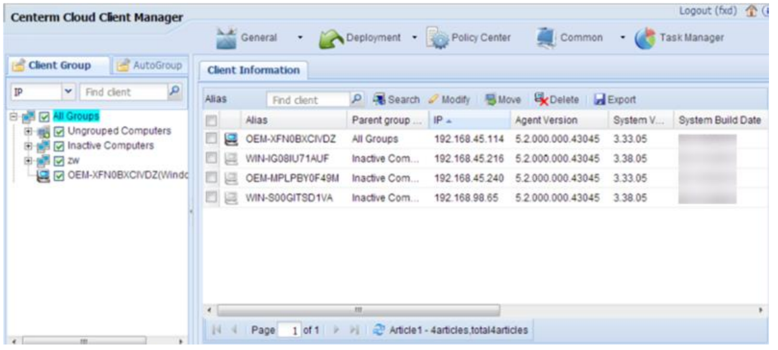
- HDC: Huawei Desktop Controller
  - As the core component of the FusionAccess software, the HDC manages desktop groups, assigns computers to users, and unassigns computers from users after receiving requests from the ITA. Additionally, it enables users to log in to computers.



- A single HDC can manage 5000 desktops. An ITA can manage multiple HDCs. A maximum of 20,000 desktops can be managed.
  - Implement and maintain the mapping between users and their virtual desktops.
  - Interacts with the WI during user access, provides access information for the user, and supports the entire user access process.
  - Interacts with the HDA in the VM and collects the VM status and access status reported by the HDA.

Virtual Desktop Management Layer(3)

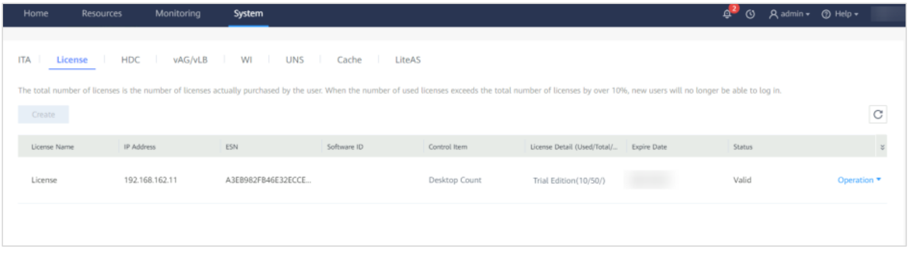
- TCM：Thin Client Management
  - The TCM is a desktop management system that allows administrators to perform routine management on TCs.



- The management server is used to centrally manage TCs, including version upgrade, status management, information monitoring, and log management.
- The management server can search for and manage TCs to be managed.

Virtual Desktop Management Layer(4)

- License
  - The License server manages and distributes licenses for the HDC.
  - The FusionAccess desktop management software mainly uses the HDP connection license. When a user connects to a VM, the user checks the license on the license server to determine whether the VM can be connected.



- The license for Huawei desktop access is controlled by the license server.
- The total number of licenses is the actual number of purchased licenses. When the number of used licenses reaches 1.1 times the total number, new users cannot log in to the desktop.

Virtual Desktop Management Layer(5)

- GaussDB
  - The GaussDB stores data for the ITA, HDC, and LiteAS.
- Backup Server
  - Backup Server is used to back up important files and data for each component.
  - Backup Server Policy:
    - Backup files on FusionAccess components are automatically uploaded to the Backup Server by using the FTPS at 01:00:00 every day.
    - Backup Server can temporarily retain the backup files generated in the latest 10 days at most.

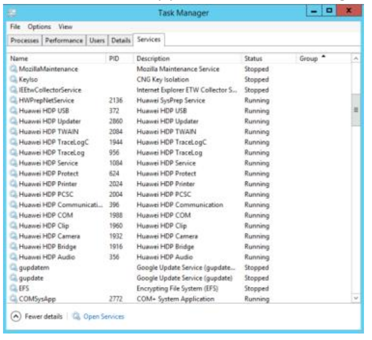
Virtual Desktop Management Layer(6)

- LiteAS:
  - Unified authentication server: the LiteAS manages and authenticates desktop users and desktop user groups who access FusionAccess.
- AUS
  - The AUS is used to upgrade the HDA. Install and configure the AUS on FusionAccess so that FusionAccess can upgrade the HDA properly.
- Cache
  - Cache server: the Cache is a high-performance key-value database that provides efficient and fast data read and write.

- FusionAccess uses the LiteAS for authentication and authorization by default. Also, you can configure a Windows AD domain on FusionAccess for authentication and authorization by performing the operations in this section. You can configure a maximum of 20 Windows AD domains.

Core Components of Desktop VMs-HDA

- HDA：Huawei Desktop Agent is a type of desktop agent software installed on VMs. VMs interact with desktop management components through the software.
- To connect a TC (SC) to a VM using the HDP protocol, the HDA must be installed on the VM.
- HDA is a series of desktop connection services that support TCs (SCs) using virtual machines.



HUAWEI

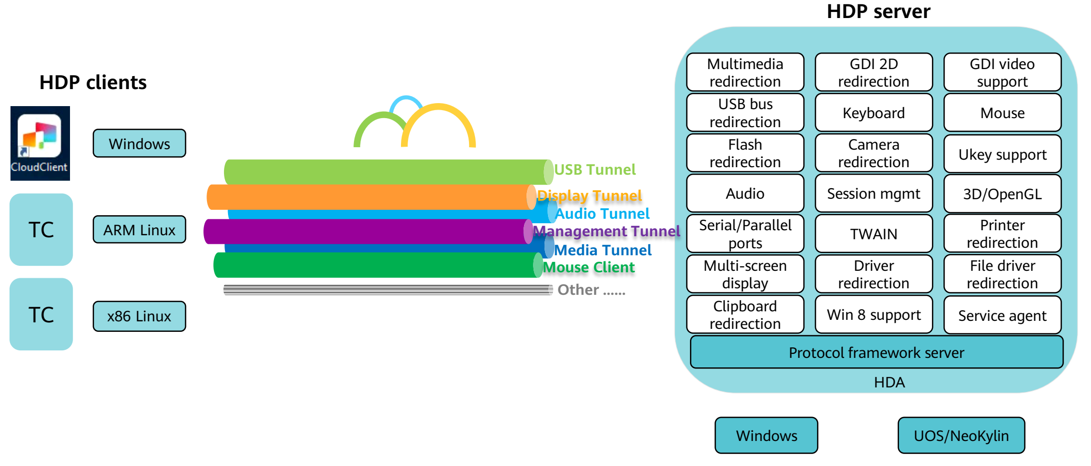
Contents

Huawei Desktop Protocol

- Huawei Desktop Protocol (HDP) is a next-generation cloud access desktop protocol with the following features:
  - Up to 64 virtual channels. Each virtual channel bears different upper-layer application protocols.
  - Different compression algorithms can be used for different application types. HDP flexibly switches between server or local rendering as needed.
  - Smooth clear video playback
  - Lossless compression algorithms
  - High fidelity audio
  - Robust protocol management policies.

- The virtual channels ensure communication security and good user experience based on Quality of Service (QoS) priorities (for example, the keyboard and mouse virtual channel can be given the top priority).
- Hardware interfaces of chips are used to accelerate video decoding and smoothen video playback. It supports 4K video playback.
- HDP adopts lossless compression algorithms for non-natural images, and does not require transmission of repeated images. When HDP is used to display non-natural images, such as characters, icons, and OA desktops, the peak signal to noise ratio (PSNR) of HDP exceeds 50,000 dB, and the structural similarity (SSIM) reaches 0.999955, providing close-to-lossless video display quality.
- HDP automatically detects voice scenarios, implements denoising when detecting noises, supports transparent voice transmission on TCs, provides more clear sound in real time, and accurately restores sound. The perceptual evaluation of speech quality (PESQ) is over 3.4.
- Multiple protocol management policies are available. It provides independent channel policies for different users and user groups to ensure communication security.

HDP Architecture



Common Desktop Protocols(1)

- ICA/HDX
  - Citrix Independent Computing Architecture (Citrix ICA) is one of the most popular virtual desktop protocols. In addition to complete functions, ICA provides the following functions:
    - Support for a wide range of mobile terminals.
    - Network protocol independence. ICA supports TCP/IP, network basic input/output system (NetBIOS), and Internet Packet Exchange/Sequenced Packet Exchange (IPX/SPX).
    - ICA supports XenServer, vSphere and Hyper-V virtualization platforms.
    - ICA requires little bandwidth, so it can be used in networks of poor quality (for example where there is high latency).
  - High Definition Experience (HDX) is an enhanced edition of ICA. HDX improves user experience with video, audio, multimedia, and 3D services. HDX supports H.264.

- ICA is the core of Citrix, connecting the platform application client operating environment and remote terminals. The I/O data (such as data about mouse, keyboard, image, sound, port, printing) of the former is redirected to the I/O devices of the latter through 32 ICA virtual channels. This provides the same user experience as using local applications.

Common Desktop Protocols(2)

- PC over IP (PCoIP)
  - PCoIP was developed by Teradici for high-end graphics design. In 2008, VMware joined Teradici in developing PCoIP to develop its own virtual desktop infrastructure (VDI) solution VMware View.
    - PCoIP works closely with the hardware. PCoIP allows data encoding and decoding and graphics processing to be implemented by dedicated hardware resources, so CPU resources freed up for other uses. Monitors equipped with PCoIP display chips are provided.
    - PCoIP is based on UDP. UDP cannot ensure reliable transmission, but it does not require the three-way handshake that TCP does for complex verification and data restoration, so it is faster and more appropriated for multimedia transmission.
    - PCoIP does not support redirection of peripherals, such as serial and parallel ports. Some TC vendors provide port redirection plug-ins to make up for this.

- PCoIP compresses and transmits user sessions as images and transmits only the changed parts, ensuring efficiency even in a low-bandwidth environment. PCoIP supports a resolution of 2560 x 1600 on multiple screens and a maximum of four 32-bit screens, and the Clear Type font.
- Unlike TCP-based protocols such as RDP or ICA/HDX, PCoIP is based on UDP. Why UDP? TCP requires a three-way handshake for verification, which makes it not applicable to the WAN environment. Online streaming media platforms such as Xunlei Kankan and PPLIVE use UDP to maximize the use of network bandwidth and ensure smooth video playback. UDP is simple and efficient, and is usually used to provide real-time services such as VoIP and video conferencing.
- PCoIP compresses and transmits user sessions as images and transmits only the changed parts, ensuring efficiency even in a low-bandwidth environment. In the WAN environment, PCoIP is adaptive and can fully utilize network bandwidth resources.
- PCoIP is a typical host-end rendering protocol with good compatibility. The line speed affects the quality of the image. With a low-speed line, PCoIP transmits a lossless image to the client. As the line speed increases, PCoIP gradually displays high-definition images. PCoIP not only supports VMware solutions, but also supports hardware encoding and decoding on blade PCs and rack workstations equipped with Teradici host cards.

Common Desktop Protocols(3)

- Simple Protocol for Independent Computing Environments (SPICE)
  - SPICE is a virtual desktop protocol developed by Qumranet. Later, it was purchased by Red Hat who provides it as an open protocol. After years of community development, SPICE is maturing.
  - SPICE is good for video services, largely because video is compressed using a Kernel-based Virtual Machine (KVM), which puts less pressure on the guest OS. SPICE uses lossless compression to provide an HD experience, but that also means it needs a lot of bandwidth.

- SPICE is a high-performance, dynamic, and adaptive telepresence technology, providing the same user experience as using local PCs. SPICE is designed and created for Red Hat Enterprise edition users to remotely access virtual desktops.
- It uses a multi-layer architecture to meet the diverse multimedia requirements of desktop users. SPICE aims to realize intelligent access of the available system resources (such as CPUs and RAM) on client devices and virtual hosts. As a result of the access, the protocol dynamically determines whether to present the desktop application on the client device or the host server to provide the optimal user experience regardless of network conditions.
- SPICE provides the optimal customer experience and has huge market potential. It is favored by Chinese virtualization vendors, such as Shenzhen Jing Cloud, CloudTop Network Technology, and NaCloud Era. Virtual desktops based on SPICE have earned the trust of customers.

Common Desktop Protocols(4)

- RDP/RemoteFX
  - Remote Desktop Protocol (RDP) is a Microsoft protocol which was developed by Citrix. RDP provides few functions and is mainly used for Windows. Mac RDP clients and Linux RDP clients RDesktop are now available as well. The latest RDP version supports printer redirection, audio redirection, and clipboard sharing.
  - RemoteFX is an enhanced edition of RDP. RemoteFX supports virtual graphics processing units (vGPUs), multi-point touch, and USB redirection.

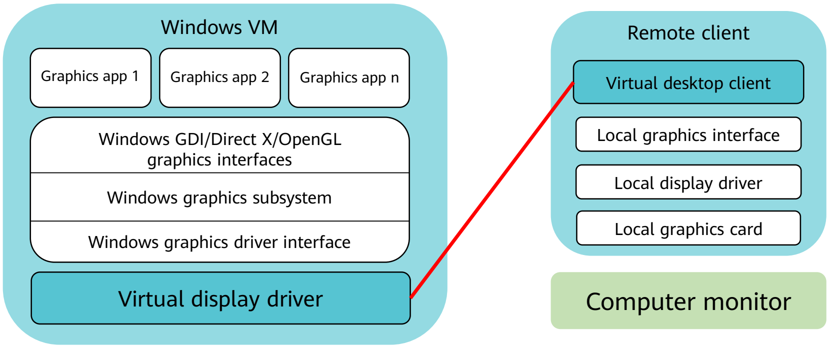
- In RDP, any authorized terminal can be a terminal server. Client can log in to the server and use the corresponding resources (including software and hardware). After the protocol is upgraded, client can even use the local resources (including the printer, audio playback, disks, and hardware interfaces). All calculations are performed on the server. The client only needs to process network connections, receive data, display interfaces, and output device data. In China, virtualization vendors that use the RDP include Beijing Fronware and Xi'an Realor.

Comparison of Common Desktop Protocols

Feature	PCoIP	ICA	RDP	SPICE	HDP
Transmission bandwidth	High	Low	High	Medium	Low
Image display	High	Medium	Low	High	High
Two-way audio support	Low	High	Medium	High	High
Video support	Low	Medium	Medium	High	High
Peripheral support	Low	High	High	Medium	High
Transmission security	High	High	Medium	High	High

HDP - 2D Graphics Display Technology(1)

- For remote display, screens of servers are captured using OS interfaces, and the screen captures are displayed on clients after processing.



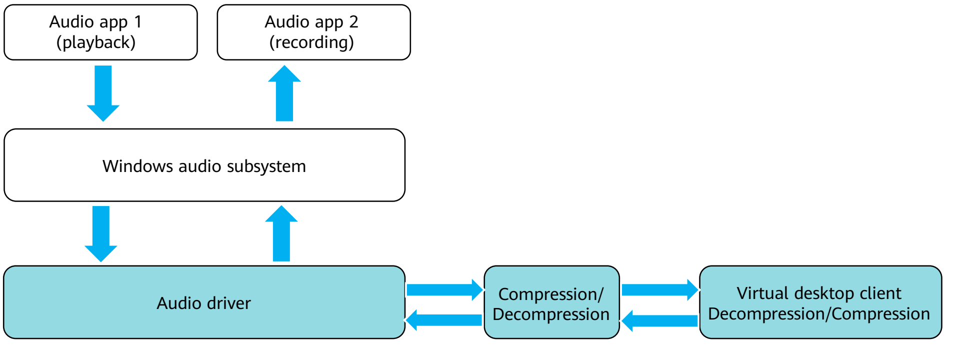
- As shown in the figure, in OS software layers, the display driver interacts with the graphics card. The upper-layer systems need to use the display driver to interact with the graphics card. Screen captures are transferred from the display driver to the graphics card of the remote TC to implement remote display.

HDP - 2D Graphics Display Technology(2)

- Key Display Technologies of HDP
  - Lossless compression for non-natural images: Non-natural images, such as text, Windows frames, and lines within images, are identified automatically and lossless compression applied. Natural images, like photos, are compressed at an appropriate rate.
  - No transmission of redundant image data: To save bandwidth, HDP identifies what image data has changed and only transmits the changes.
  - Support for multiple image compression algorithms: The most appropriate compression algorithm is selected based on different image characteristics and use cases.

HDP - Audio Technology(1)

- The HDP server simulates an audio driver on a VM. The audio driver interacts with the Windows audio subsystem (audio engine).



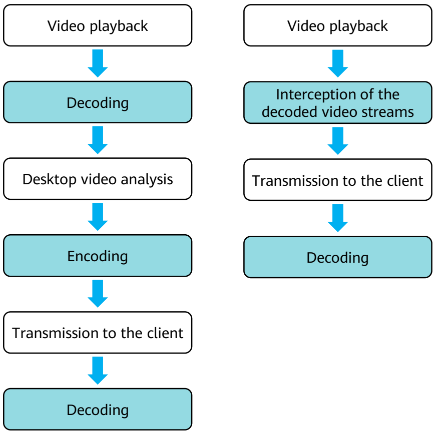
- During audio playback, the audio driver transmits audio data received from the Windows audio subsystem to the desktop protocol client after compression, and the client plays the audio after decoding. During audio recording, the client transmits local recording data to the server after compression, the server decodes the data, and the audio driver returns the data to the Windows audio subsystem. Audio is sensitive to latency, so latency must be controlled in the whole process.

HDP - Audio Technology(2)

- Key Audio Technologies of HDP
  - High-fidelity music compression algorithm: Sound scenarios are automatically identified. A voice compression optimized for VoIP used for voices and professional high-fidelity music codecs are used for music.
  - Automatic denoising: A denoising algorithm is used for VoIP to ensure excellent voice quality even in noisy environments.
  - Low latency: Voice content is transmitted transparently on TCs to avoid buffering, reduce latency, and ensure real-time performance for voice communications.
  - High sound quality: A default 44.1 kHz sampling rate ensures quality audio.
  - Stereo mixing: All VM audio inputs and outputs can be mixed.

HDP - Display Technology(1)

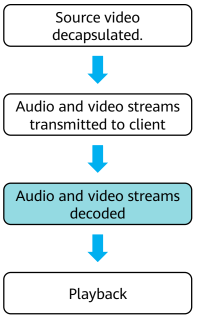
- Currently, Huawei Desktop Protocol supports two types of video playback:
  - Video recoding: Multimedia playing on the server is re-coded before being transmitted to the client for decoding and display.
  - Video redirection: Video streams on the server are captured and transmitted directly to the client for decoding and display.



- According to the figures, video redirection is more efficient because no resources are required for video decoding and re-coding on the server. However, this method has some disadvantages:
  - In method 1, the player running in the desktop VM consumes a large number of CPU resources for decoding videos. More CPU resources are consumed when the video area is encoded. As a result, VM density of a server is reduced. Moreover, dynamically detecting the video area is technically challenging. Usually, the image change area where the refresh rate exceeds a certain frame rate is detected as the video area.
  - In method 2, video code streams to be decoded are intercepted on the server only and then transmitted to the client for decoding and display, which consumes less CPU resources of the server. The multimedia redirection technology for Media Player is a popular client decoding technology. However, this technology is not popular in China because the Media Player is rarely used in China. The multimedia redirection technology for other players is emerging.

HDP - Display Technology(2)

- HDP supports 4K video playback. Source video files are transmitted from the server to the client, where they are decapsulated and decoded for playback.
  - After decapsulation, audio and video streams are played back directly to avoid putting pressure on network bandwidth.
  - Less demand is placed on the server.
  - TCs can be used for 4K video playback.



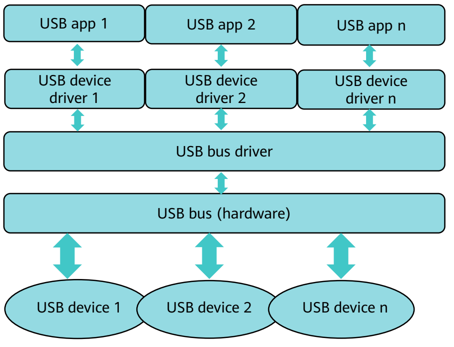
HDP - Display Technology(3)

- Key Video Technologies of HDP
  - Intelligent identification: The display server automatically distinguishes between video data and common GDI data. H.264 or MPEG2 is then used to encode the video and the TC takes care of the decoding.
  - Dynamic frame rate: To ensure smooth playback, the playback frame rate is adjusted on the fly based on the network quality.
  - Video data auto-adaptation: To ease pressure on the CPU and improve user experience, video streams are adjusted automatically based on the display resolution and the size of the video playback window.
  - Multimedia redirection: TC hardware is used for decoding, dynamic traffic adjustment, 4K video playback, to reconnect automatically if the network connection is dropped. The TC hardware can provide smoother playback than Citrix ICA.
  - Application sensitivity: Commonly-used video playback and image processing software (like Photoshop) are optimized based on customer demands.

HDP - Peripheral Redirection(1)

- In virtual desktops, peripherals on the TC/SC side are mapped to a remote desktop using desktop protocols. Depending on how they are used, peripheral technologies are classified as either port redirection or device redirection:
  - Port redirection: The port protocols are redirected to the OSs of the remote desktops. Examples include USB port redirection, serial port redirection, and parallel port redirection.
  - Device redirection: The device application protocols are redirected to the OSs of the remote desktops. Examples include camera redirection and TWAIN redirection.

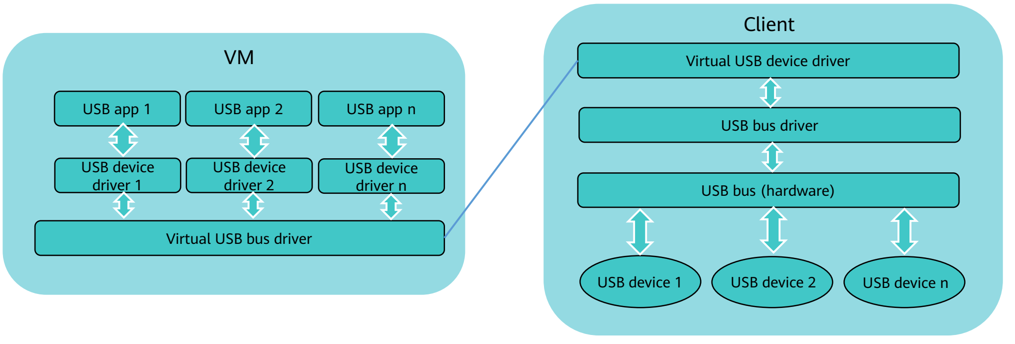
HDP - Peripheral Redirection(2)



Working principles of USB devices on PCs

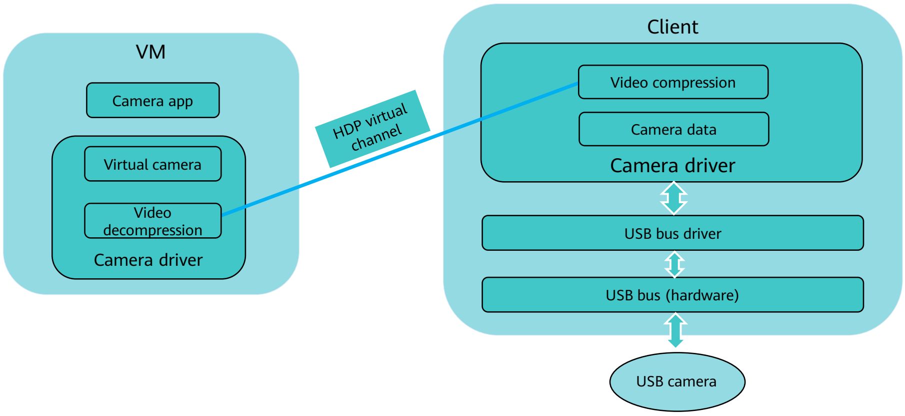
- The preceding figure shows that the USB bus driver is essential for enabling USB devices to work normally at the software layer. When an application needs to use a USB peripheral, it must interact with the USB device driver. The USB device driver relies on the USB bus driver to exchange data with the USB device and interacts with hardware using the bus driver as an agent.

HDP - Peripheral Redirection(3)



- The preceding figure shows the USB port redirection mode. A virtual USB bus driver is embedded in the VM and client respectively to use the remote physical USB bus driver. USB device drivers are installed and running on the VM and interact with the virtual USB bus driver. The USB device drivers and applications on the VM are not aware that the USB devices are running on a remote TC. USB port redirection is irrelevant to specific devices and applications and provides good compatibility because USB ports are redirected to desktop VMs. However, without compression and preprocessing at the device driver layer, graphics applications that are sensitive to network latency, such as applications of scanners and cameras, require a high bandwidth. In this case, the device redirection technology must be used.

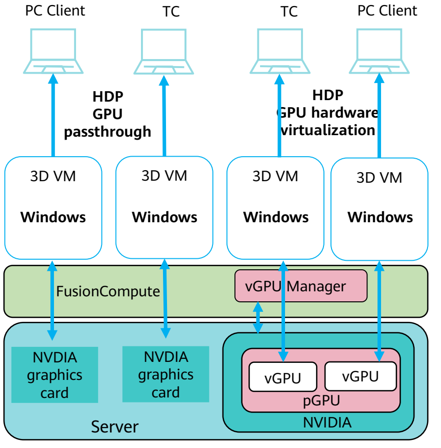
HDP - Peripheral Redirection(4)



- Device redirection works at the device driver layer. A device driver is embedded in the TC and VM. The collected data is compressed and preprocessed by the device driver on the TC. The processed data is transmitted to the device driver on the VM using a desktop protocol. After being restored by the device driver on the VM, the data is transmitted to applications for processing.
- If cameras are redirected in USB redirection mode, dozens of Mbit/s bandwidths are required, which cannot meet the requirements of commercial use. Therefore, specific optimizations are performed for USB peripherals to ensure that USB peripherals can be commercially used in the virtual desktop system. We can use the camera redirection mode in the preceding figure to optimize cameras.
- As shown in the preceding figure, the client obtains camera data (bitmap data or YUV data) using an application-level interface, compresses the data using a video compression algorithm (such as H.264), and sends the compressed data to the server. The server decodes the camera data and provides the data to the application through the virtual camera. Compared with USB bus redirection mode, this camera redirection mode reduces bandwidth tenfold.

HDP - 3D Graphics Display Technology

- Huawei HD graphics desktop supports multiple HD graphics software products. There are three types of 3D graphics technologies used:
  - GPU Passthrough
  - GPU Hardware Virtualization
  - Graphics Workstation Management



- GPU Passthrough:
  - GPU passthrough is used to bind a VM to each GPU, and each VM uses a GPU exclusively and accesses the GPU by using a driver. Equipped with GPU passthrough and HDP, the Huawei GPU passthrough HD graphics processing feature enables users to remotely access VMs to use GPU 3D acceleration. GPU passthrough is compatible with various types of graphics cards and supports the latest 3D applications that comply with DirectX and OpenGL.
- GPU Hardware Virtualization:
  - Equipped with the vGPU technology, GPU hardware virtualization is used to virtualize a NVIDIA GRID graphics card into several vGPUs. Each vGPU is bound to a VM and the VM accesses the vGPU just like it accesses the physical GPU. By using the FusionCompute virtualization platform, the Huawei GPU hardware virutalization HD graphics processing feature allows virtualizing one physical GPU into several vGPUs. Each vGPU is bound to a VM and the VM exclusively uses the vGPU. In this way, multiple VMs share a physical GPU, improving resource usage. A GPU can be shared by a maximum of 32 users and supports 3D applications that comply with the latest DirectX and OpenGL standards.
- Graphics Workstation Management:
  - Graphics workstations are dedicated computers that specialize in graphics, static images, dynamic images, and videos. Graphics workstations are widely used in 3D animation, data visualization, CAD, CAM, and EDA that require high graphics processing capability. Graphics workstation management allows graphics workstations to be featured in FusionAccess and enables users to access the graphics workstations to use GPU 3D acceleration using HDP. It is compatible with various types of graphics cards and supports the latest 3D applications that comply with DirectX and OpenGL.

Contents

Application Scenarios of Desktop Cloud

High security

Secure office

- Enterprise security R&D
- Finance/Legal High-Sensitive Positions
- e-Government intranet

Standardization

Public desktop

- Meeting Room/Common Work Area
- Training Center/E-Reading Room
- Customer Service Center

Personalization

Common office

- Enterprise common office
- R&D O&M
- Human resources/logistics management
- E-Government extranet

Designer

GPU graphics

- Professional 3D graphics design
- High-precision audio and video processing
- Industrial simulation
- New media operation

Secure Office: Intranet and Extranet Isolation Allows On-Demand Usage(1)

- Logical isolation and physical isolation are supported.
- A TC supports two gigabit network adapters (logically isolated). Because the desktop cloud of the office network and the desktop cloud of the service network are physically isolated, users need to use TCs with dual network ports to access the two desktop clouds at the same time. TC network adapter 1 connects to the office network, and TC network adapter 2 connects to the service network. The DVI port on a TC supports dual-screen extended display. Users can log in to and operate two virtual desktops at the same time. When a TC is connected to one monitor, the two virtual desktops can be switched by pressing the Minimize/Maximize button. When a TC terminal is connected to two monitors, each monitor can display a virtual desktop. The two monitors can be operated simultaneously.

Secure Office: Intranet and Extranet Isolation Allows On-Demand Usage(2)

- One TC and a set of mouse and keyboard are used. A network cable switcher (physically isolated) is added at the front end of the TC. The switcher is used to control whether the TC connects to the intranet or extranet desktop. However, the switchover is performed through the switcher. Therefore, the virtual desktop of only one VM can be displayed at a time.

Public Desktop: Pooled Desktops, No Fixed Relationship, and Automatic Recycling

- Public desktops in pooling mode can be used for standard office in conference rooms, embassies, and audio-visual classrooms.
- A public desktop refers to a desktop user who is not fixed. After the desktop is used up, the system automatically reclaims the desktop.
- Supports restart and restoration.
- To upgrade and patch VMs, the administrator only needs to update the system base disk in the storage and rebuild all desktops in batches.

HUAWEI

- Public desktop characteristics:
  - No fixed user is assigned. Users use public desktops temporarily or in turn.
  - Virtual desktops are displayed without entering the username and password.
  - Virtual desktops are vulnerable to viruses and Trojan horses due to frequent access to the Internet.
  - VMs are usually batch restarted or shut down.
  - The installed software can be batch updated.
  - Maintenance is simple.

A Standard Office: Application in Government and Enterprises

- Users and VMs are configured in 1:1 ratio. Each user has an independent desktop. The full copy desktop cloud is isolated based on VMs. Each desktop has an independent system disk and data disk. The full copy desktop cloud features high security, strong customization, and good performance experience. Various peripherals are supported. Users can flexibly expand storage space. The user experience is the same as that of traditional PCs.

- This scenario has the following characteristics:
  - 1:1 dedicated desktop (full copy)
  - Independent system disk and data disk space for each user
  - Supports personalized application installation requirements.
  - Users' personal data can be stored.

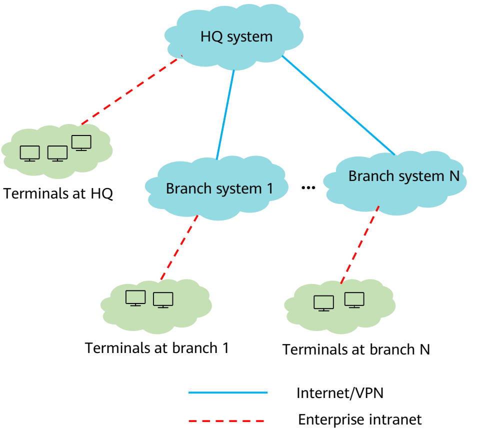
Professional Design: High-Performance GPU Cloud Desktops Unleash Creativity and Productivity

- GPU-designed desktop: The desktop cloud solution provides 3D graphics rendering capabilities for end users.
- Huawei GPU virtualization graphics desktop uses the NVIDIA GPU hardware virtualization technology to virtualize one physical GPU card into multiple vGPU cards. Each vGPU card is bound to a VM, and the VM exclusively uses one vGPU. Multiple VMs share a physical GPU card to share GPU resources.

- Features: This scenario supports multiple HD graphics software, including mainstream 3D design software such as Catia, Creo, and AutoCAD, simulation software such as Ansys, Abaqus, and Matlab, and common GIS and omnimedia video editing software. It can meet the HD image processing requirements of customers in multiple industries, such as engineering, manufacturing, oil and gas, automobile, medical, gaming, and media assets.
- Huawei HDP uses the dedicated low-latency remote display technology to capture virtual desktop images using graphics card hardware to reduce latency. In addition, Huawei HDP uses the image recognition technology to identify desktop images and uses different compression algorithm to efficiently compress and encode virtual desktops and send them to TCs. This greatly improves user experience when users interact with VMs.

Branch Offices

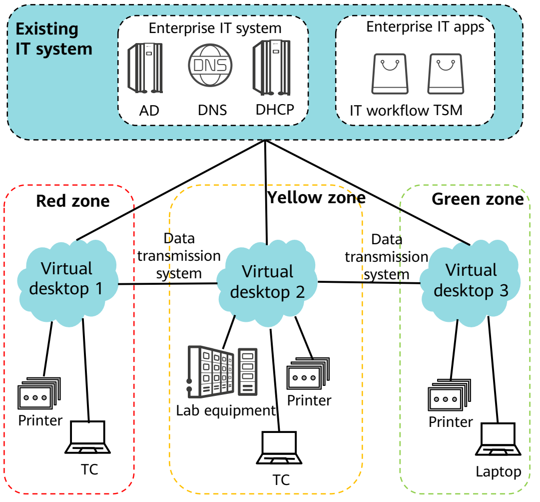
- Introduction
  - Virtual desktops are often deployed in branch offices to improve user experience.
- Benefits
  - Network costs are reduced.
  - Service continuity is ensured.
  - O&M and management are centralized.



- Only management data is transmitted through the network between the headquarters and branch offices. Local traffic is used for VM remote desktops. This eliminates the need for network bandwidth. The minimum bandwidth required is 2 Mbit/s, and the latency is less than 50 ms. If virtual desktops are deployed in a centralized manner, high requirements are put on network bandwidth and latency for connecting to the virtual desktops remotely. If video and audio services are required, higher requirements are put on network bandwidth and latency. Deploying virtual desktops in the branch office reduces the cost in building remote private networks and provides good VM user experience.
- In addition, desktop management software is deployed in branch offices to ensure service reliability. Even if the WAN is disconnected, the VMs to which users have logged in can still run properly and branch services are uninterrupted.
- An O&M system is deployed in the headquarters to implement centralized O&M of virtual desktops in the headquarters and branch offices.

Office Automation

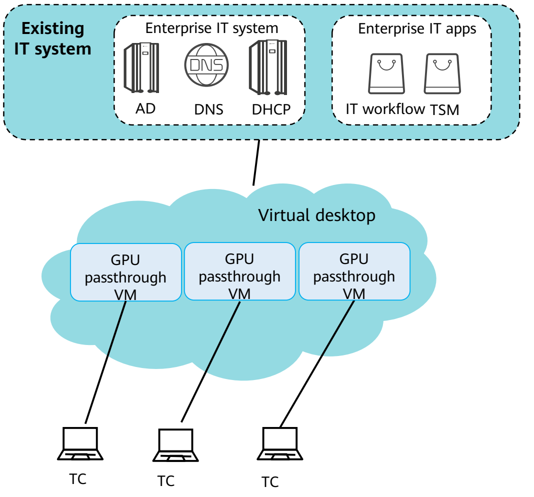
- Introduction
  - FusionAccess allows users in an enterprise to handle work such as email processing and document editing, on a cloud computing platform and with high information security.
- Benefits
  - Less investment and a smoother transition
  - High information security
  - Deployment that is simple and flexible



- FusionAccess can smoothly connect to enterprises' existing IT systems, allowing enterprises to make the most of their prior investments. For example, an enterprise can use the existing AD system to authenticate desktop users, and users can process existing IT workflows in FusionAccess. In addition, FusionAccess can assign IP addresses to virtual desktops using DHCP or resolve desktop domain names using an enterprises' existing DNS server.
- FusionAccess uses various authentication and management mechanisms to ensure information security in workplaces.
  - Users can use virtual desktops only after passing AD authentication.
  - Data is stored by confidentiality in red, yellow, and green zones, which are separated from each other. Information in the red zone is top secret under the highest level of strict control. Information in the yellow zone is confidential and under a medium level of control. The green zone stores the least confidential information and is accessible by mobile users and from outside the enterprise.
- The zone-based security control meets the security management requirements of most enterprises. It is easy and flexible to deploy.
- Huawei has deployed about 70,000 desktops in its headquarters and branch offices and has successful OA desktop projects in commercial use worldwide.

GPU Desktop Professional Graphics

- Introduction
  - GPU virtual desktops provide powerful graphics processing capabilities in addition to CAD drawing and animation rendering.
- Benefits
  - Reused physical GPU resources
  - Reduced costs
  - Centralized data management



- Graphics software usually needs to invoke 3D instructions to achieve the optimal image display. The commonly used instructions are D3D and OPENGL that require the support of GPUs.
- FusionAccess provides GPU passthrough and GPU hardware virtualization for graphics processing software.
- Lower Costs:
  - With FusionAccess, users do not need to purchase new PCs or servers, or even pay for software license upgrade. That is, instead of investing in assets that are depreciating, resources are directed towards other strategic investments.
- Secure, Guaranteed, and Flexible:
  - FusionAccess ensures that users can log in to the system using the Microsoft Remote Desktop Service protocol and restricts users' access to specific folders, applications, and files. This means that users can control data security. In addition, the virtual desktop will run on a dedicated server reserved for the user's company. This protection, together with centralized management of configuration files, helps companies improve compliance to ensure the security and privacy of user data.
- Centralized Data Management:
  - Data is centrally stored on a hosted desktop, helping users find important documents more quickly.

Quiz

1. Which of the following are mainstream virtual desktop protocols?
   A. HDP
   B. RDP
   C. ICA
   D. SIP
2. FusionAccess is a virtual system used to create and provision virtual desktops.
   A. True
   B. False

- Answers:
  - ABC
  - A

Summary

- Having completed this course, you have learned some concepts related to FusionAccess (especially the definitions and functions of each component), the structure of a VDI and an IDV, and some common desktop protocols.
- In the following courses, you will learn about the planning, installation, deployment, and service provisioning of FusionAccess.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Acronyms and Abbreviations

AD: Active Directory

AUS: AccessAgent Update Server

DNS: Domain Name Server

DHCP: Dynamic Host Configuration Protocol

GPU: Graphics Processing Unit

HDA: Huawei Desktop Agent

HDC: Huawei Desktop Controller

HDP: Huawei Desktop Protocol

HDX: high-definition experience desktop protocol of Citrix. It is an enhanced version of ICA.

Citrix ICA: Citrix Independent Computing Architecture

Acronyms and Abbreviations

IDV: Intelligent Desktop Virtualization

ITA: IT Adapter

PCoIP: PC over IP, a virtual desktop protocol jointly developed by VMware and Teradid.

RDP: Remote Desktop Protocol (Microsoft)

SC: Software Client

SPICE: Simple Protocol for Independent Computing Environments (Red Hat)

TC: Thin Client

TCM: Thin Client Management

UNS: Unified Name Service

Acronyms and Abbreviations

vAG: Virtual Access Gateway

VDI: Virtual Desktop Infrastructure

vLB: Virtual Load Balancer

VM: Virtual Machine

WI: Web Interface

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

FusionAccess: Planning and Deployment

Foreword

- FusionAccess installs various management components on VMs. These components are vAG, vLB, ITA, WI, GaussDB, and HDC. FusionAccess also interacts with other components on the live network: Microsoft Active Directory (AD) domain controller components, Domain Name Service (DNS) responsible for domain name resolution, and Dynamic Host Configuration Protocol (DHCP).
- This FusionAccess course describes both the component planning and overall installation process and the initial configuration process.

Objectives

- On completion of this course, you will be able to:
  - Understand the FusionAccess deployment scheme.
  - Describe the functions and basic features of Windows AD.
  - Understand the installation and configuration process of AD, DNS, and DHCP.
  - Master the FusionAccess initial configuration process.

Contents

FusionAccess Deployment Scheme

Deployment Scheme	Description
All-in-one deployment	All components (ITA/GaussDB/HDC/Cache/WI/License/vAG/vLB/LiteAS/VNCProxy)are deployed on the same VM. In dual-node deployment mode, the two active/standby VMs must be deployed on different CNAs.
Standard deployment	The IT Adapter (ITA), GaussDB, Huawei Desktop Controller (HDC), Cache, Web Interface (WI), License, and LiteAS components are deployed on the same VM. The virtual access gateway (vAG), virtual load balance (vLB), and VNCProxy components are deployed on another VM, respectively.
UNS deployment	The Unified Name Service (UNS) enables a unified domain name to be used to access multiple FusionAccess systems. If this feature is required, use the UNS deployment solution.

- All-in-one deployment (user quantity < 500). This scheme applies to scenarios involving only intranet user access. (This course focuses on this scenario). Extranet/public network user access scenarios are not discussed in this course.
- Standard deployment (500 ≤ user quantity ≤ 10,000).
- UNS deployment, the UNS deployment scheme is not described in this course.

All-in-one deployment

Component	Parameter	Description
ITA/GaussDB/HDC/Cache/WI/ License/vAG/vLB/LiteAS/VNCProxy	OS	Select EulerOS 2.8 64bit for the ARM architecture. Select EulerOS 2.5 64bit for the x86 architecture.
	Specifications	8 vCPUs, 16 GB memory, 60 GB system disk, and 2 NICs (The second NIC is optional) **NOTE:** Only the first NIC is added during VM creation. The second NIC must be added after the components are installed and configured.
	Deployment mode	**Dual-node deployment** **All components are deployed on the same VMs in active/standby mode. The active and standby VMs reside on different Computing Node Agent (CNA) nodes.**

HUAWEI

- The first NIC belongs to the service plane, and the second NIC belongs to the management plane.

Standard deployment (1)

Component	Parameter	Description
ITA/GaussDB/HDC/Cache/WI/ License/LiteAS	OS	Select EulerOS 2.8 64bit for the ARM architecture. Select EulerOS 2.5 64bit for the x86 architecture.
	Specifications	8 vCPUs, 16 GB memory, 60 GB system disk, and 2 NICs (The second NIC is optional) **NOTE:** Only the first NIC is added during VM creation. The second NIC must be added after the components are installed and configured.
	Deployment mode	**Dual-node deployment** **All components are deployed on the same VMs in active/standby mode. The active and standby VMs must be deployed on different CNA nodes.**
(Optional) vAG	OS	Select EulerOS 2.8 64bit for the ARM architecture. Select EulerOS 2.5 64bit for the x86 architecture.
	Specifications	4 vCPUs, 4 GB memory, 40 GB system disk, and 2 NICs (The second NIC is optional) **NOTE:** Only the first NIC is added during VM creation. The second NIC must be added after the components are installed and configured.
	Deployment mode	**The vAG is separately deployed and two vAGs are deployed by default. One vAG is added when the quantity of users increases by 500 each time.** **All vAGs must be deployed on different CNA nodes.**

Standard deployment (2)

Component	Parameter	Description
(Optional) vLB	OS	Select EulerOS 2.8 64bit for the ARM architecture. Select EulerOS 2.5 64bit for the x86 architecture.
	Specifications	8 vCPUs, 4 GB memory, 40 GB system disk, and 2 NICs (The second NIC is optional) **NOTE:** Only the first NIC is added during VM creation. The second NIC must be added after the components are installed and configured.
	Deployment mode	**The vLB is separately deployed on two VMs in active/standby mode.** **The active and standby VMs must be deployed on different CNA nodes.**
(Optional) VNCProxy	OS	Select EulerOS 2.8 64bit for the ARM architecture. Select EulerOS 2.5 64bit for the x86 architecture.
	Specifications	More than 4 vCPUs, 4 GB memory, and 40 GB system disk
	Deployment mode	**The VNCProxy is separately deployed on two VMs in active/standby mode.** **The active and standby VMs must be deployed on different CNA nodes.**

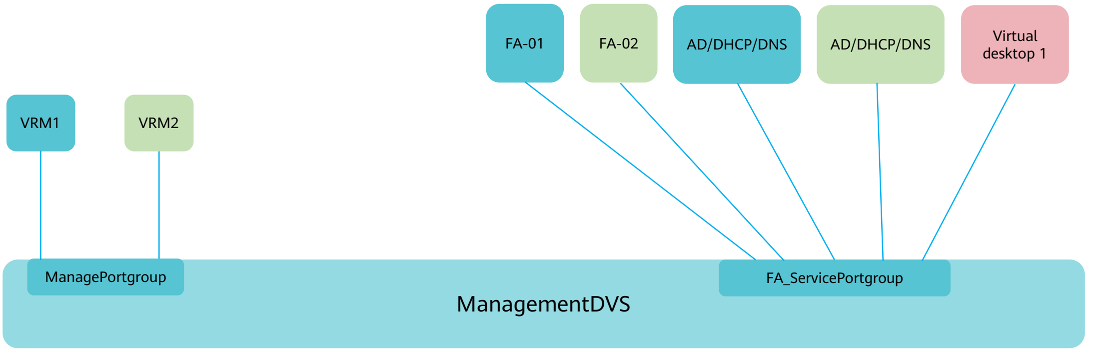
- Other optional components include AUS, TCM, Backup Server, and DHCP.
- Deploy the Thin Client Management (TCM) on a dedicated VM because its port conflicts with those of the ITA, WI, UNS, and vLB.
- Deploy the WI and UNS on different VMs because their ports conflict.
- In standard deployment, deploy the vLB and UNS on different VMs.
- When creating VMs where management components are to be installed, you are advised to use high-performance storage instead of low-performance storage, such as NL-SAS and SATA disks.
- Deploy the License on a dedicated VM if multiple FusionAccess systems share a license.

Network Plane and Component Deployment Plan

- Port group for the management plane NICs of infrastructure VMs:
  - **ManagementDVS** and a port group whose VLAN ID is **0** are automatically created in the process of establishing a virtual platform. This port group can be configured for the management plane NICs.

Port group for the service plane NICs of infrastructure VMs (1)

- If the service plane and the management plane belong to **the same network segment**, you are advised to create a port group for the service plane NICs on ManagementDVS.
- The following figure uses the **all-in-one deployment** of FusionAccess components as an example.

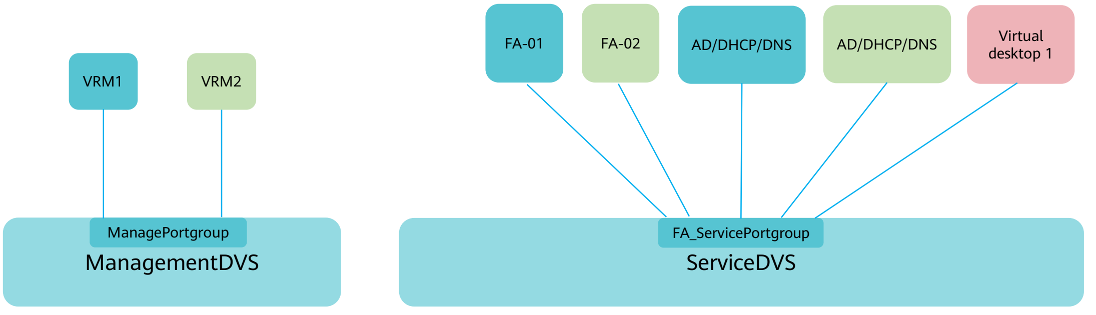


FA-01 and FA-02：ITA/GaussDB/HDC/Cache/WI/License/vAG/vLB/LiteAS/VNCProxy

- The preceding recommendation is prerequisite. The service plane and the management plane belong to the same network segment. In this case, you are advised to create a port group for the service plane NIC on the ManagementDVS.
- Deploy all management nodes in active/standby mode at commercial sites.

Port group for the service plane NICs of infrastructure VMs (2)

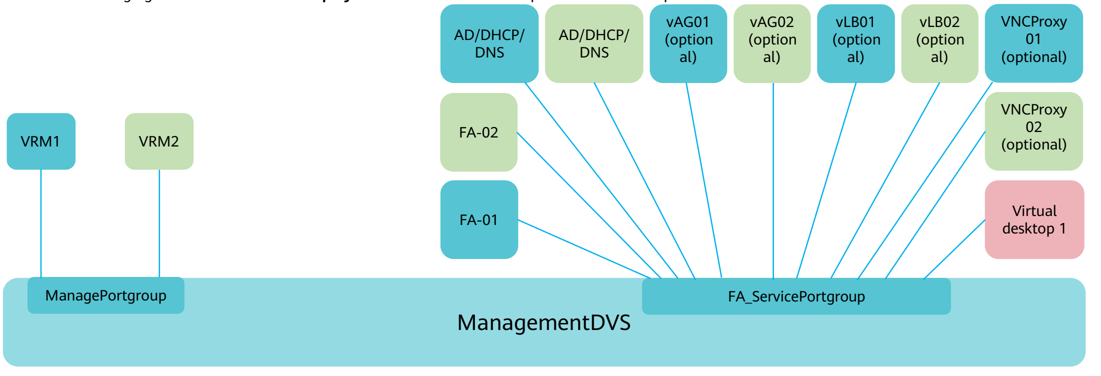
- If the management plane and service plane belong to **different network segments**, create a port group for the service plane NICs on the service DVS.
- The following figure uses the **all-in-one deployment** of FusionAccess components as an example.



FA-01 and FA-02：ITA/GaussDB/HDC/Cache/WI/License/vAG/vLB/LiteAS/VNCProxy

Port group for the service plane NICs of infrastructure VMs (3)

- If the service plane and the management plane belong to **the same network segment**, you are advised to create a port group for the service plane NICs on ManagementDVS.
- The following figure uses the **standard deployment** of FusionAccess components as an example.

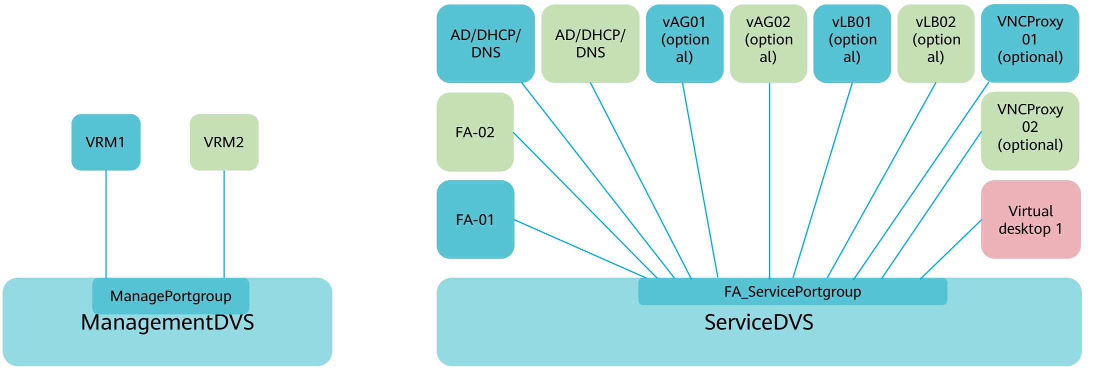


FA-01 and FA-02：ITA/GaussDB/HDC/Cache/WI/License/LiteAS

HUAWEI

Port group for the service plane NICs of infrastructure VMs (4)

- If the management plane and service plane belong to **different network segments**, create a port group for the service plane NICs on the service DVS.
- The following figure uses the **standard deployment** of FusionAccess components as an example.



FA-01 and FA-02：ITA/GaussDB/HDC/Cache/WI/License/LiteAS

Contents

Active Directory (AD)

- Definitions
  - ADs store network resource information for query and usage. Such information includes user accounts, computer information, and printer information.
  - AD is a directory service. It stores, searches, and locates objects and manages computer resources centrally and securely.
  - AD provides directory management for medium- and large-sized networks on Microsoft Windows Server.
- Content
  - The directories in a Windows Server AD domain store user accounts, groups, printers, shared directories, and other objects.
- Function
  - AD manages and protects user accounts, clients, and applications, and provides a unified interface to secure intranet information.

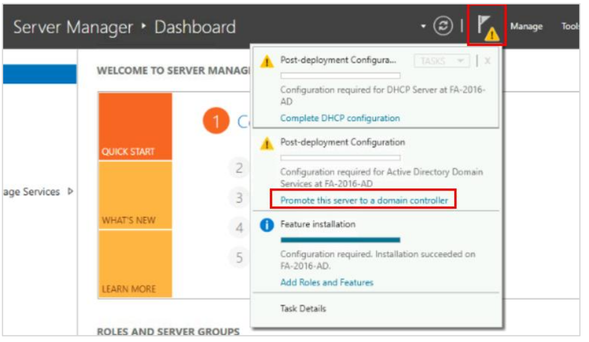
- AD is a sophisticated service component for Windows Server OS. AD processes network objects, including users, groups, computers, network domain controllers, emails, organizational units, and trees in organizations.
- The AD provides the following functions:
  - Basic network services, including DNS, Windows Internet Name Service (WINS), DHCP, and certificate services.
  - Server and client computer management: manages server and client computer accounts, and applies policies to all servers and client computers that are added to the domain.
  - User service: manages user domain accounts, user information, enterprise contacts (integrated with the email system), user groups, user identity authentication, and user authorization, and implements group management policies by default.
  - Resource management: manages network resources, such as printers and file sharing services.
  - Desktop configuration: allows the system administrator to centrally configure various desktop configuration policies, such as restricting portal functions, application program execution features, network connections, and security configurations.
  - Application system support: supports various application systems, including finance, human resources, email, enterprise information portal, office automation, patch management, and antivirus systems.

AD Objects

- The smallest management unit of an AD is an object (a group of attributes). In an AD domain, the following basic objects are organized in the tree structure:
  - Domain controller: stores network domain controllers (equipment contexts).
  - Computer: stores computer objects added to the network domain.
  - Default account group (Builtin): stores in-house account groups.
  - User: stores user objects in the AD.
  - Organization Unit (OU): stores AD objects (users, groups, and computers) to reflect the AD organizational structure. This design enables objects to be managed using the organizational structure.

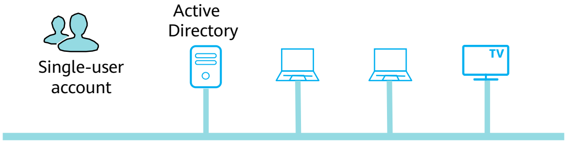
Domain Controller

- The directory data of the AD domain service is stored in domain controllers. There can be multiple domain controllers in a domain, and each are equally important. Data is synchronized between the domain controllers, so each domain controller stores a copy of the same AD database.



Domain User Account

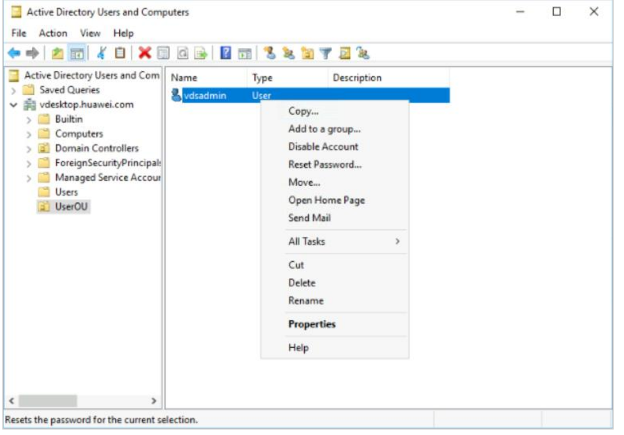
- Domain user accounts are created on domain controllers. This account is the only credential needed for domain access and is stored in the AD database of the domain as an AD object. When a user logs in to a domain from any computer in the domain, the user must provide a valid domain user account, which will be authenticated by the domain controller.



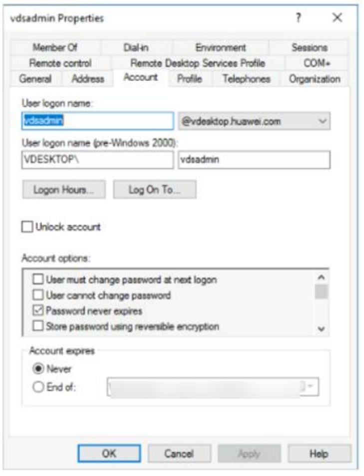
HUAWEI

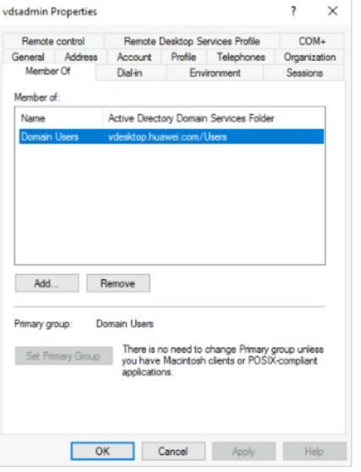
Common Operations on Domain Accounts

- Add to group
- Disable account
- Reset password
- Move
- Delete
- Rename

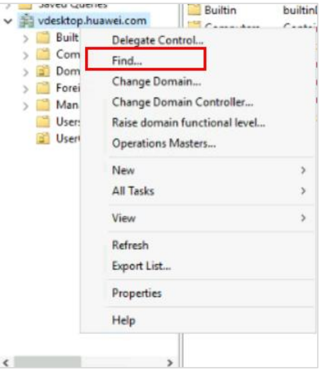


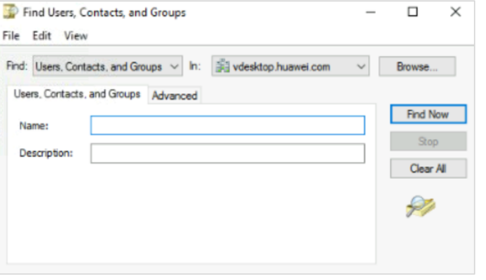
User Domain Account Properties





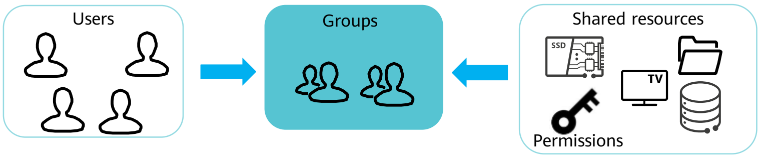
Finding a User Domain Account





User Group

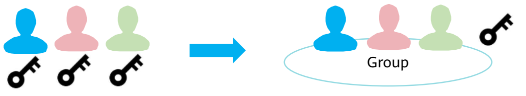
- A group is a logical collection of user accounts.
- User groups manage accounts using in-domain resource access permissions.



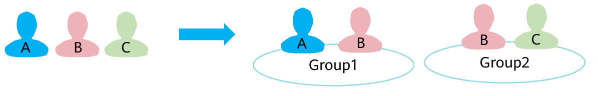
HUAWEI

Groups in the AD

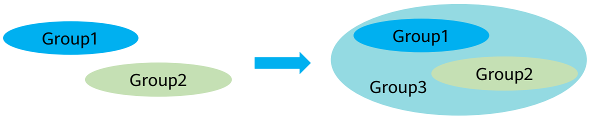
- Groups simplify the allocation of resource permissions.



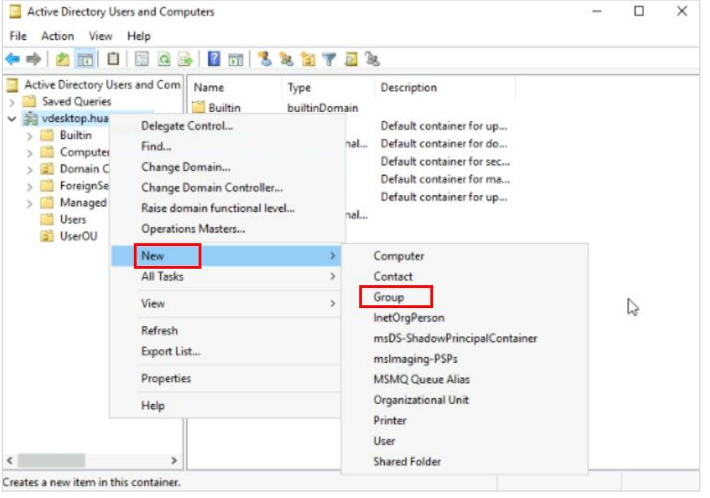
- A user can join multiple groups.



- A group can be nested in another group.

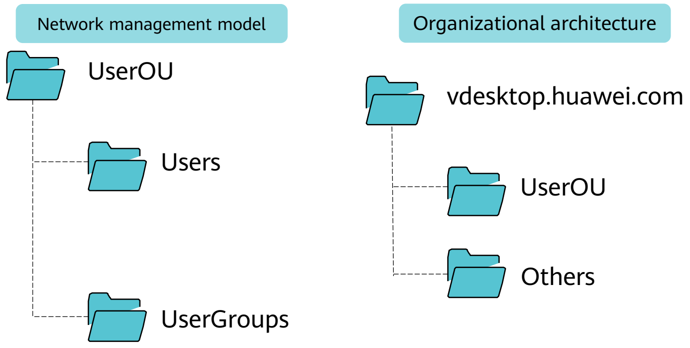


Creating a User Group



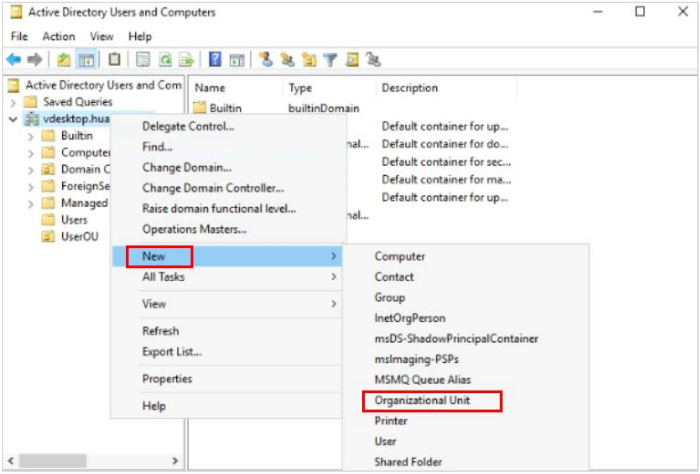
Organization Unit (OU)

- An OU organizes objects logically as required by an organization.
- To delegate OU management and control rights, assign the permissions of the OU and its objects to one or more users or groups.



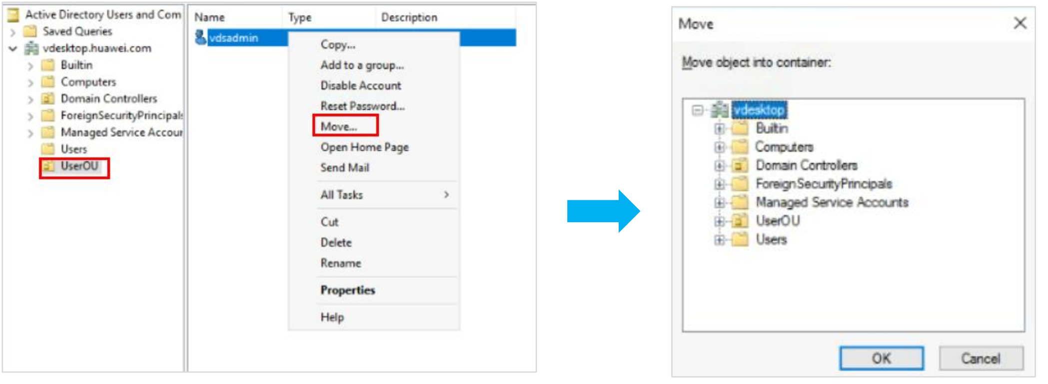
- To facilitate management, add Computers to the created VM OU.

Creating an OU



- OUs cannot be created in common containers.
- Common containers and OUs are at the same level and do not contain each other.
- OUs can be created only in domains or OUs.

Moving AD Objects Between OUs



- After a user account is moved, the permissions assigned to the user account remain unchanged.
- The user account uses the group policy of the new OU.

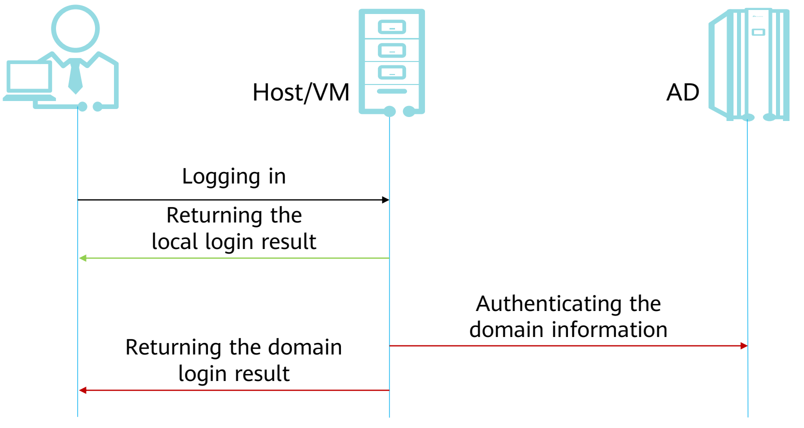
User Groups vs. OUs

- Similarity
  - OUs and user groups are AD objects.
- Differences
  - A user group can contain only accounts.
  - An OU can contain accounts, computers, printers, and shared folders.
  - OUs have a group policy function.

Domains vs. OUs

- Similarities
  - OUs and domains are AD logical structures.
  - Both OUs and domains are the management unit of users and computers. They contain AD objects and configure group policies.
- Differences
  - Users can log in to a domain but not an OU.
  - Domains are created before OUs.
  - OUs can exist in domains, but domains cannot exist in OUs.
  - A domain is at a higher level than an OU.

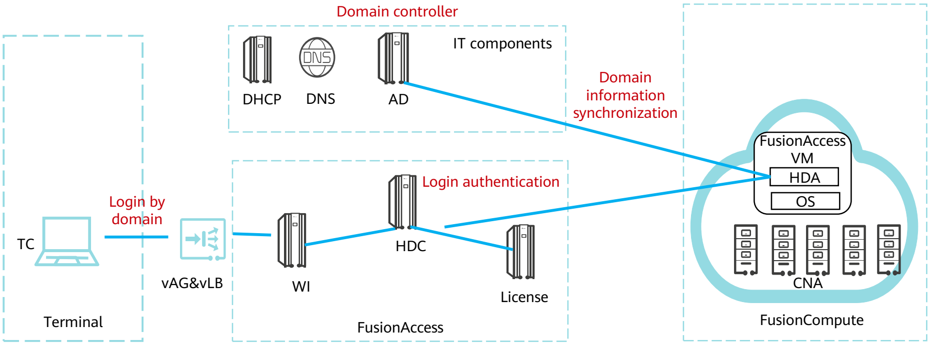
Adding a Computer to an AD Domain



- If a user attempts to log in to the host, the system obtains the username and password, processes them with the key mechanism, and compares them with the key stored in the account database. If a match is found, the user is allowed to log in to the computer. If not, the login fails.
- If a user attempts to log in to a domain, the system verifies whether the account information stored in the domain controller database is consistent with the information provided by the user. If yes, the user is allowed to log in to the domain.

Typical AD Desktop Applications

- A user logs in to a desktop using domain username.
- The HDC sends a request to the AD for user information authentication.
- A user VM synchronizes the domain information to a Domain Controller.



- The user VM synchronizes information with the domain controller during user login or forcibly using the AD server.

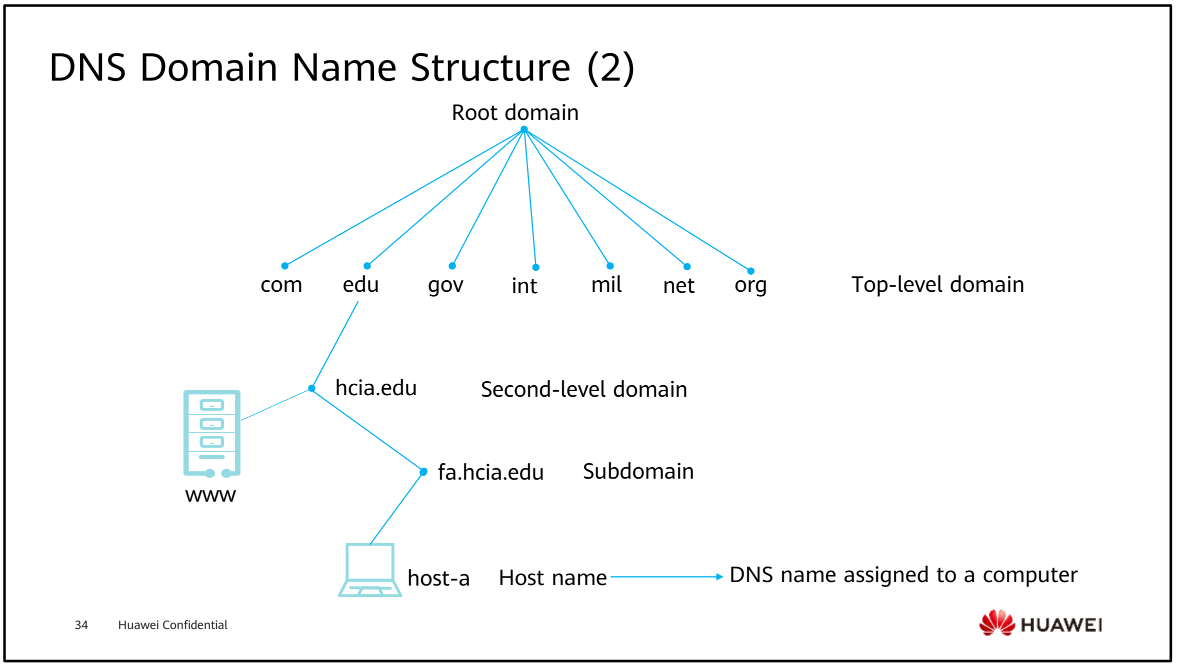
Domain Name System (DNS)

- DNS is a distributed database that converts IP addresses and domain names for network access.
- DNS advantages:
  - Users can access the network with easy-to-remember character strings, instead of IP numbers.
  - DNS cooperates with the domain controller.
  - A domain controller registers its role with the DNS server so that other computers can find its host name, IP address, and domain controller.

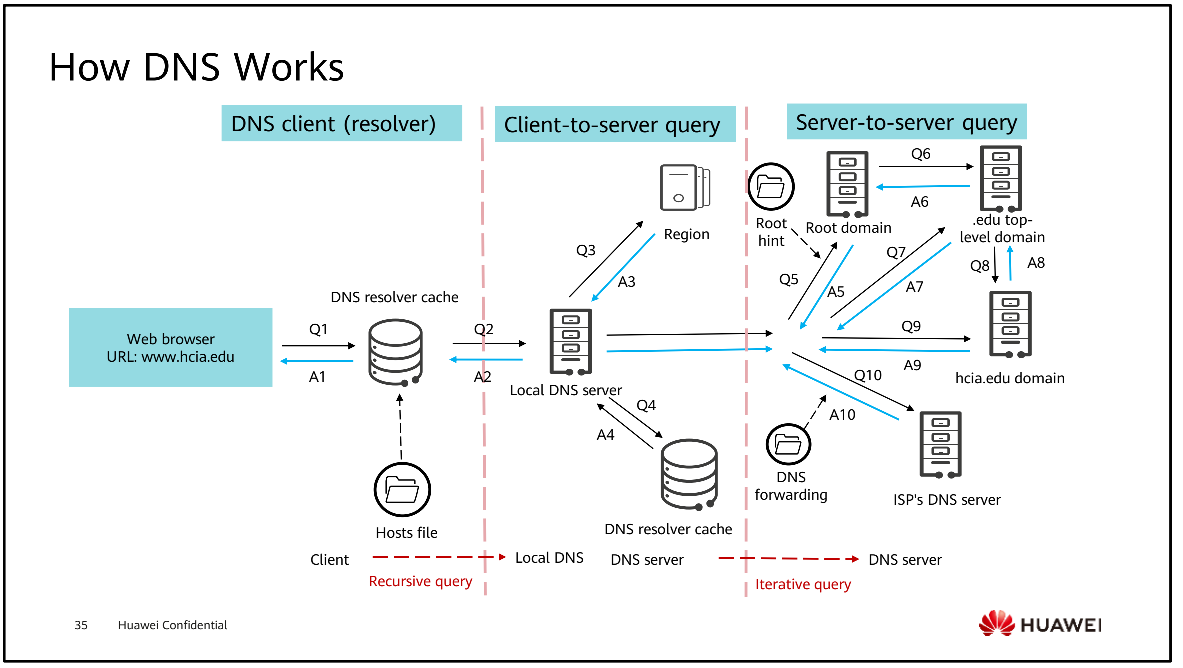
- DNS history
  - DNS technology was created in 1983, with the original technical standards being released in RFC 882. The DNS technical standards were revised in RFC 1034 and RFC 1035 released in 1987, followed by the abolishment of RFC 882 and RFC 883. The later RFC versions have not seen any changes on the DNS technical standards.

DNS Domain Name Structure (1)

- The DNS domain name management system includes: the root domain, top-level domain, second-level domain, subdomain, and host name. The structure of the domain name is like an inverted tree: The top of the structure is the roots and the highest level, while the leaves identify the lowest level.



- Common domains with three characters:
  - com: indicates a commercial organization.
  - edu: indicates an educational organization.
  - gov: indicates a governmental organization.
  - int: indicates an international organization.
  - mil: indicates a military site.
  - net: indicates a network.
  - org: indicates other organizations.
- Country (region) domains with two characters:
  - cn: indicates the Chinese mainland.
  - tw: indicates Taiwan (China).



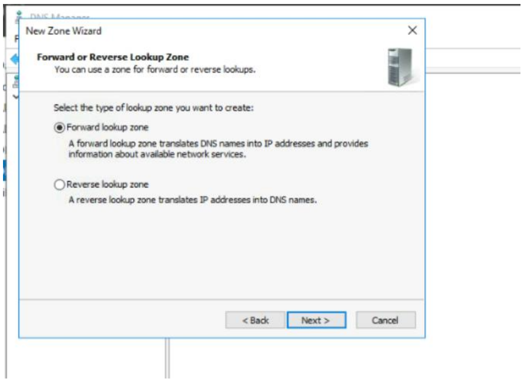
- Recursive query
  Recursive query is a query mode of the DNS server. In this mode, after receiving a request from a client, the DNS server must return an accurate query result to the client. If the DNS server does not store the queried information locally, it queries other servers and sends the query result to the client.
- Iterative query
  Iterative query is the other query mode of the DNS server. In this mode, after receiving a request from a client, the DNS server does not directly return the query result but notifies the client of the IP address of another DNS server. The client then sends a request to the new DNS server. The procedure repeats until the query result is returned.
- Terms
  - hosts file: provides the mapping table between IP addresses and host names in static mapping mode, which is similar to the ARP table.
  - Domain: A domain is in the format of **abc.com** and can be divided into multiple zones, such as **abc.com** and **xyz.abc.com**.
- The following shows three ways for the host of **www.abc.com** to query the IP address of the server of **www.xyz.abc.com**:

- Recursive query:
  - Step 1: Query the IP address of a host of **www.xyz.abc.com** in the hosts static file and DNS resolver cache.
  - Step 2: If the query in step 1 fails, query the IP address in the local DNS server (domain server). That is, query the IP address in the region server and server cache.
  - Step 3: If the query in step 2 fails, query the IP address in the DNS server responsible for the top-level domain (.com) based on the root hints file.
  - Step 4: The root DNS server queries the IP address in the region server of **xyz.com**.
  - Step 5: The DNS server of **www.xyz.abc.com** resolves the domain name and returns the IP address to the host that sends the request along the same route.
- Iterative query:
  - Step 1: Query the IP address of a host of **www.xyz.abc.com** in the hosts static file and DNS resolver cache.
  - Step 2: If the query in step 1 fails, query the IP address in all the region servers at the current level on the local DNS server (domain server).
  - Step 3: If the query in step 2 fails, query the IP address in all the region servers at the upper level. Repeat the query until the root DNS server.
  - Step 4: After reaching the root DNS server, query the IP address downwards until the IP address is found. Combination of iterative query and recursive query:

- Recursive query is a layer-by-layer query mode. For multi-layer DNS structure, the mode is inefficient. Therefore, the combination of iterative query and recursive query is generally used.
    - Step 1: Query the IP address of a host of **www.xyz.abc.com** in the hosts static file and DNS resolver cache.
    - Step 2: If the query in step 1 fails, query the IP address in the local DNS server (domain server). That is, query the IP address in the region server and server cache.
    - Step 3: If the query in step 2 fails, query the IP address in the DNS server responsible for the top-level domain (.com) based on the root hints file.
    - Step 4: The root DNS server directly returns the IP address of the DNS server in its zone to the local server, without querying in the region server of **xyz.com**.
    - Step 5: The local DNS server returns the result to the host sending the request.

DNS Forward Lookup

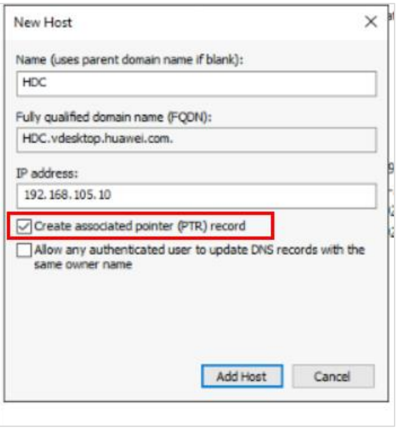
- DNS forward lookup needs a forward lookup zone - the zone where forward lookup is used in the DNS domain name space. Forward lookup resolves the domain names provided by DNS clients to IP addresses.



HUAWEI

Adding a DNS Record

- After creating a forward lookup zone, create the host (host01) record for the zone. The record is used to map the DNS domain name to the IP address used by the computer.
- If you select **Create associated pointer (PTR) record** when creating a host record in the forward lookup zone, you add a pointer to the reverse lookup zone.



HUAWEI

DNS Reverse Lookup

- A reverse lookup zone needs to be established to resolve an IP address to a domain name.
- After creating a reverse lookup zone, create a record pointer for the zone. This pointer is used to map the IP address of the forward DNS domain name computer to the reverse DNS domain name.

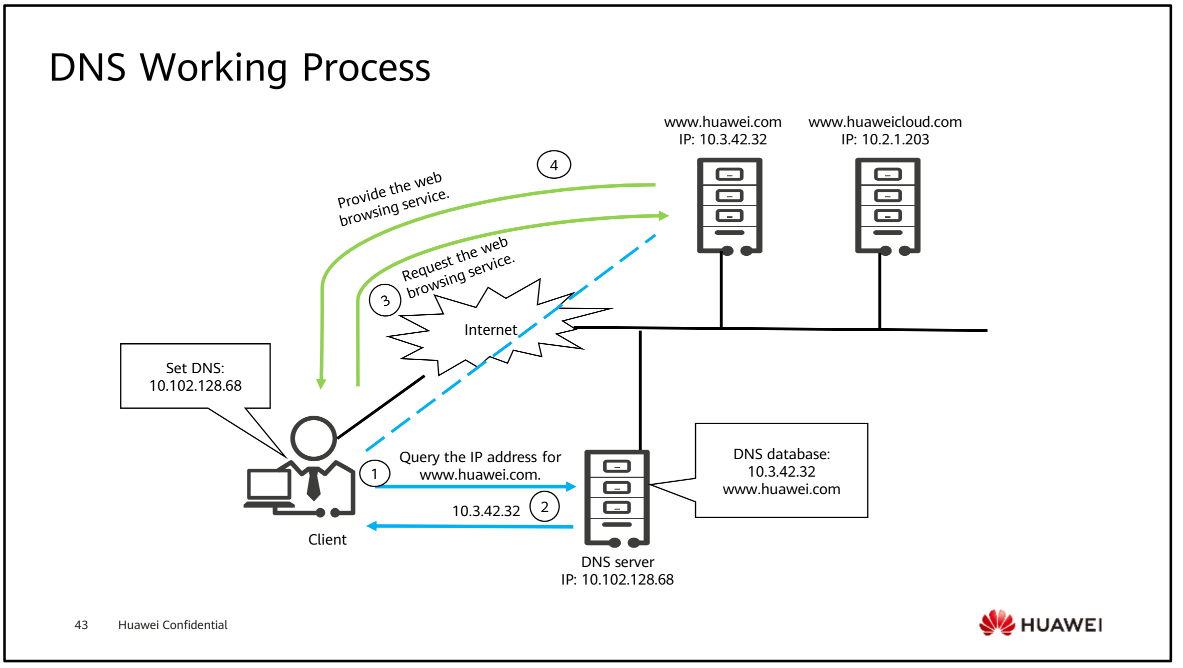
Configuring a DNS Forwarder

- Configure a DNS forwarder.
  - When a DNS client sends a domain name resolution request to the DNS server, the DNS server first tries to resolve the name. If the resolution fails, the DNS server sends a recursive query request to other DNS servers. Therefore, you must ensure that the DNS server has the forwarder function.
  - For VMs to log in to the external or public networks, you must configure DNS forwarding on the DNS server.

Client DNS Configuration

- Configure the DNS server address for clients.

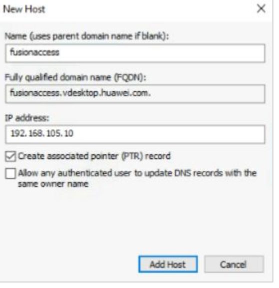
HUAWEI

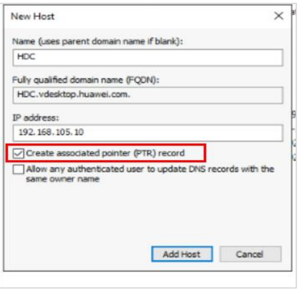


- The process of accessing **www.Huawei.com** on a client is as follows:
  - The client sends a query request to the destination DNS server to query the IP address of **www.Huawei.com**.
  - The DNS server returns the IP address of the domain name to the client.
  - The client finds the corresponding web server based on the returned IP address and accesses the web page.
  - The web server returns the information about the deployed web page to the client.

DNS Resolution in FusionAccess

- Domain name used for logging in to vLB/WI
  - To log in to VMs, users must configure the required domain names on the DNS server.
- HDC computer name
  - When registering with HDC, user VMs must use the HDC domain name to find its IP address on the DNS server for authentication.

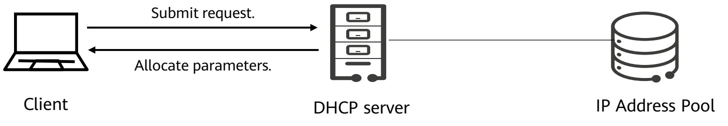




HUAWEI

DHCP

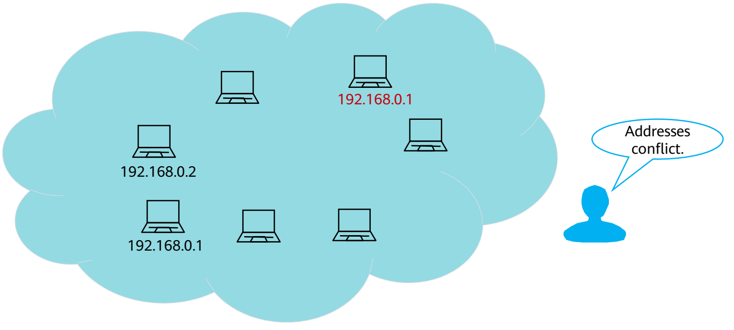
- DHCP is a communication protocol for network administrators to centrally manage and automatically assign IP addresses.
- After receiving a client request, the DHCP server provides the terminal with parameters (IP address, default gateway, and DNS server IP address).



- DHCP is a network protocol used for IP networks. It is located at the application layer of the OSI model and uses the UDP protocol. DHCP provides the following functions:
  - Automatically assigns IP addresses to users for the intranet or network service providers.
  - Centrally manages all computers for the intranet administrator.
- DHCP is a communication protocol that enables network administrators to centrally manage and automatically assign IP addresses.
- On an IP network, each device connected to the Internet must be assigned a unique IP address. With DHCP, network administrators can monitor and assign IP addresses from the central node.
- DHCP uses the concept of lease, which is also called the validity period of the computer IP address. The lease period depends on how long it takes a user to connect to the Internet in a place.

Necessities of DHCP (1)

- In larger networks, client IP addresses allocated by different users may be the same.



Necessities of DHCP (2)

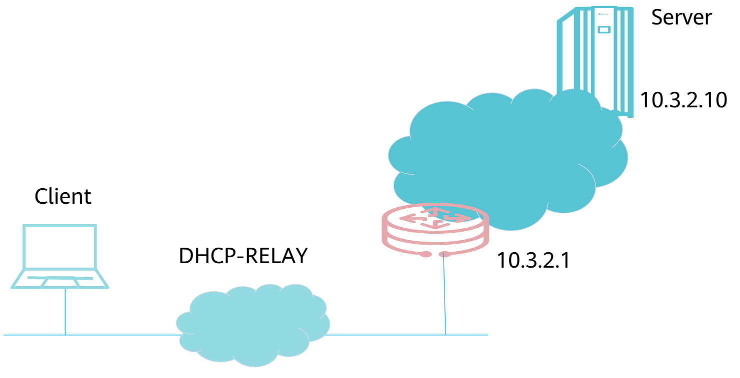
- In a TCP/IP network, each workstation must perform basic network configurations before accessing the network and its resources. Mandatory parameters include the IP address, subnet mask, default gateway, and DNS. Required information includes IP management policies.
- In larger networks, it is difficult to ensure that all hosts have correct configurations.
- To simplify IP address configuration and centralize IP address management, DHCP was designed by the Internet Engineering Task Force (IETF).

- Manual network configuration is especially difficult for dynamic networks that contain roaming subscribers and laptops. Computers are often moved from one subnet to another or out of the network. It may take a long time to manually configure or reconfigure a large number of computers. If an error occurs during the configuration of an IP host, the communication with other hosts on the network may fail.

Functions of DHCP

- Reduce errors.
  - DHCP minimizes manual IP address misconfiguration, such as address conflict caused by the reallocation of an assigned IP address.
- Simplify network management.
  - With DHCP, TCP/IP configuration is centralized and automatic. The network administrator defines TCP/IP configuration information of the entire network or a specific subnet. DHCP automatically allocates all additional TCP/IP configuration values to clients. Client IP addresses must be updated frequently. For example, a remote access client moves frequently, but frequent updates enable efficient and automatic configuration when it restarts at a new location. At the same time, most routers can forward DHCP configuration requests, so DHCP servers do not usually need to be configured on each subnet.
- Distribute network configuration information to all desktops.

DHCP Relay Switch



- If a DHCP server configures the network for the computers on another network, you can configure a DHCP-RELAY to process and forward DHCP information between different subnets and physical network segments.

Contents

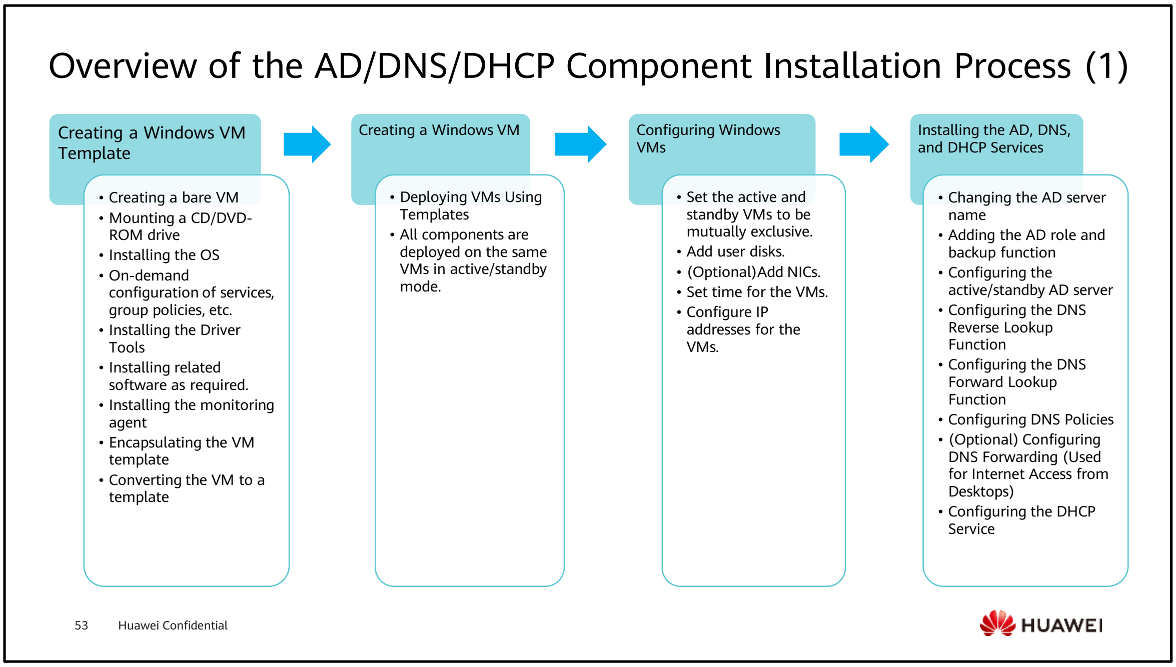
AD, DNS, and DHCP Installation Plan

Component	Parameter	Description
AD/DNS/DHCP	OS	Windows Server 2016 Standard/Datacenter 64-bit Windows Server 2019 Standard/Datacenter 64-bit
	Specifications	2 vCPUs, 4 GB memory, 50 GB system disk, and 2 NICs (The second NIC is optional) **NOTE:** Add one management plane NIC for each of the active and standby AD VMs only if the AD needs to synchronize time with the CNA where the VRM is located.
	Deployment mode	**Dual-node deployment** **The two active/standby VMs must be deployed on different CNAs.**

HUAWEI

- Huawei does not provide the Windows Server AD. You need to purchase it by yourself.
- When configuring a Windows AD VM, you need to add and initialize data disks. (This data disk is used to configure the backup path. The available disk space must be greater than 15 GB.)

Contents



- When creating VMs where management components are to be installed, you are advised to use high-performance storage instead of low-performance storage, such as NL-SAS and SATA disks.
- When using a template to deploy a VM, deselect **Generate Initial Password** on the **Customize OS** page.

Overview of the AD/DNS/DHCP Component Installation Process (2)

Creating Domain Administrator Accounts

- Creating a user domain OU
- Creating a VM OU
- Creating a domain account

Configuring Domain Administrator Accounts

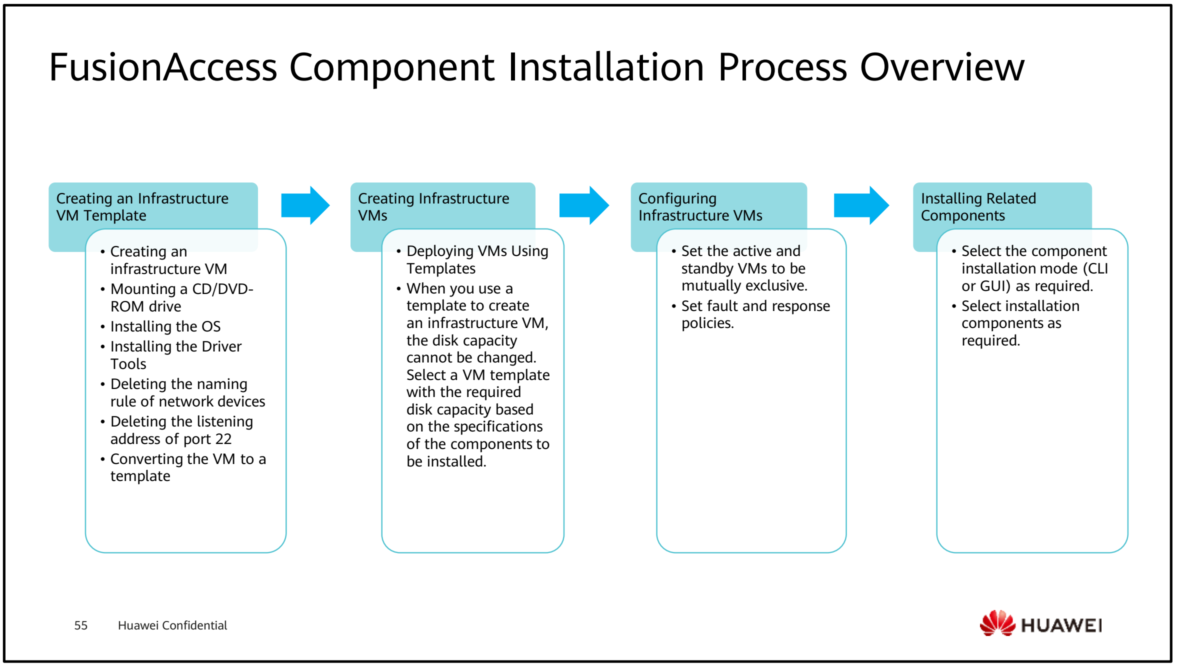
- Logging in to the active AD server.
- Configuring delegation control for the domain.
- Configuring delegation control for the OU to which the VM belongs.

Configuring Backup Paths and Remote Assistance

- Configuring backup paths
- Configuring remote assistance.

Activating the OSs of Windows VMs

- A user purchases a valid license file and activating the OS of all Windows VMs.



- An infrastructure VM template is used to quickly create VMs with the same characteristics and disk capacity. After an infrastructure VM template is created, the disk capacity cannot be changed. If infrastructure VMs with different disk capacities are required in the deployment scheme, you need to create VM templates with different disk capacities.
- The CLI mode can be used only for the all-in-one deployment solution. For other deployment solutions, use the GUI mode.

Contents

FusionAccess Initial Configuration Procedure (1)

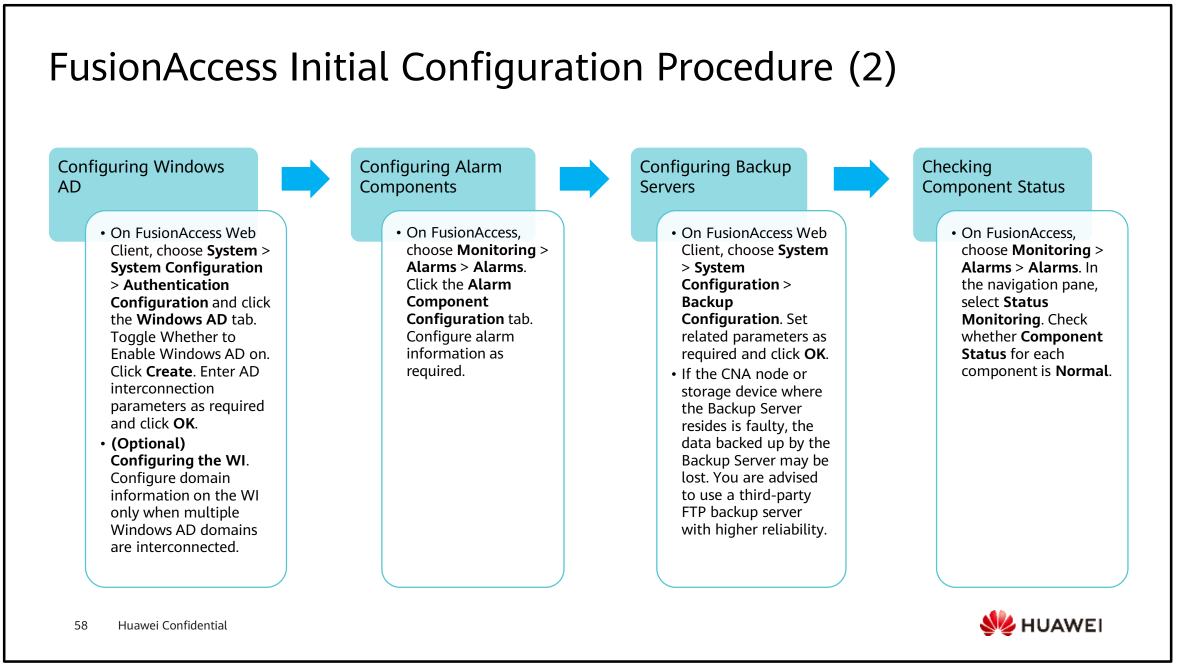
Configuring FusionAccess by Following the Wizard →
- Creating an Interface Interconnection User on FusionCompute
- Configuring the virtualization environment on FusionAccess
- (Optional) Configuring the vAG/vLB/VNCProxy
- Configuring a default policy

Configuring Time Synchronization →
- Configuring time synchronization for virtualization platforms and third-party devices
- Configuring FusionAccess time synchronization

Configuring the Self-Help Console Certificate →
- Obtaining and importing certificates
- Configuring the VNCProxy component
- Synchronizing internal communication certificates

Configuring a WI Cluster
- Configure WI cluster parameters as required.

- When the external Windows AD server is connected, ensure that the time of the external Windows AD server is the same as that of the FusionAccess server. Otherwise, Windows AD domain authentication will fail.
- If FusionCompute 8.2.0 or later is used, the self-help console function is implemented by the VNCProxy component.
- If the vAG/vLB is used as the gateway and load balancing, you need to log in to the FusionAccess page and configure WI cluster parameters.



- FusionAccess uses the LiteAS for authentication and authorization by default. Also, you can configure a Windows AD domain on FusionAccess for authentication and authorization by performing the operations in this section. You can configure a maximum of 20 Windows AD domains.
- **Enable Alarm:**
  - If you enable this function, FusionAccess will monitor the following components: Backup Server, ITA, GaussDB, License, HDC, Cache, WI, vAG, vLB, UNS, AUS, and LiteAS
  - If you disable this function, FusionAccess will not monitor the components.
- **Active DHCP IP Address and Standby DNS IP Address:** To monitor the DHCP component, configure the service plane IP addresses of the active and standby DHCP servers.
- If the AUS component is installed in the system, you need to configure the AUS on the FusionAccess GUI after the AUS component is installed to ensure that the system works properly.

Quiz

1. Which of the following components are deployed on Linux infrastructure VMs in the FusionAccess solution?
   A. ITA
   B. AD
   C. HDC
   D. WI
2. When deploying Linux infrastructure VMs, the WI and vLB/vAG components are deployed on the same VM.
   A. True
   B. False

- Answers:
  - ACD
  - A

Summary

- This course has taught you both FusionAccess component planning and overall installation and initial configuration.
- Subsequent certification courses will introduce desktop provisioning and O&M in the FusionAccess environment.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Acronyms and Abbreviations

- ARM: Advanced Reduced Instruction Set Computing Machines
- CNA: Computing Node Agent
- DVS: Distributed Virtual Switch
- IETF: Internet Engineering Task Force
- OS: Operating System
- OU: Organization Unit
- PTR: Pointer Record
- vNIC: Virtual Network Interface Card

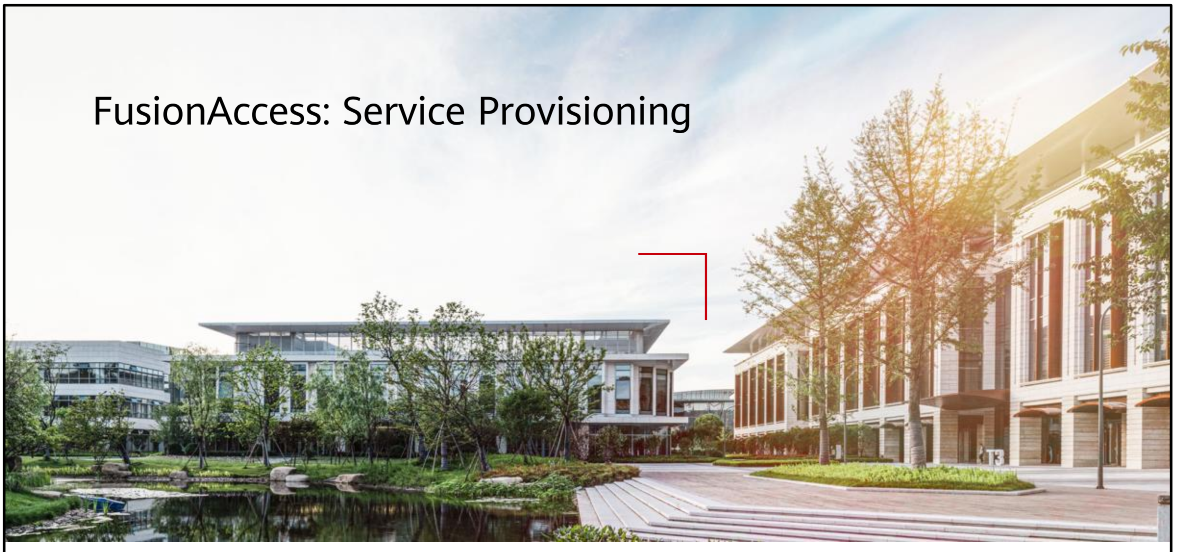
Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

FusionAccess: Service Provisioning



HUAWEI

Foreword

- Clone technology is important for virtual desktops. It enables templates to be batch-deployed on desktops. Clone technology can be divided into full copy and linked clone.
- This course introduces full copy and linked clone, differences between different virtual desktops, and virtual desktop provisioning process in Huawei FusionAccess.

Objectives

- On completion of this course, you will be able to:
  - Learn principles of full copy and linked clone.
  - Distinguish full copy, linked clone, and QuickPrep.
  - Master process for creating a VM template.
  - Master process for provisioning a virtual desktop.

Contents

Background of Clone

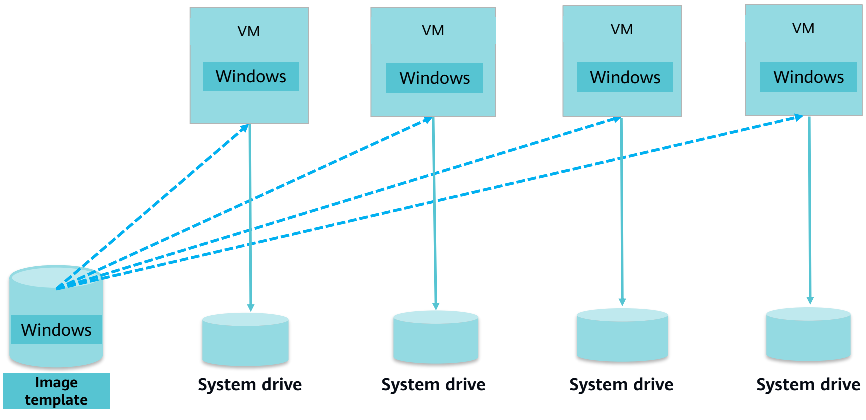
- Virtual desktop technologies enable the batch provisioning and O&M of office desktops, and make enterprise IT management easier. The most important one is the clone technology. Administrators can easily clone a parent VM/template to more VMs, facilitating IT management and O&M. The cloned VMs have the same OS, application systems, data, and documents as the parent VM.
- Clone is divided into full copy and linked clone. Based on users' requirements, QuickPrep derived from full copy.

Computer Templates

- A computer template is dedicated to deploying computers that are exactly the same operating system as the computer template. Administrators can directly use computer templates to build computers without installing operating systems and applications.
- The creation process for computer templates:
  - Create a bare VM, install the OS, software on which the OS depends and customized software on the VM by using the OS ISO file, convert the VM into a computer template.
  - Convert an existing computer into a template, namely, copying each volume of the computer to generate a new template.
  - FusionCompute allows users to export created computer templates to local PCs and import existing computer templates to FusionCompute.

- Administrators need to specify whether to enable the computers to start automatically, and can adjust computer specifications, including CPUs, memory, NICs, drives, and whether to enable HA. If administrators do not adjust computer specifications, the specifications of the created computers are the same as those of the computer template by default.
- When administrators use a computer template to create computers, the data on the drives of the computer template is copied to the drives of the created computers after administrators select appropriate data storage for the new computers. The appropriate data storage must connect to the same node as the data storage for the template.

A Full Copy Desktop



Independent computer that is created using a source computer (not join a domain) template.

- Users can save data changes (such as installed software) on computers.
- The target computer has its own CPU, memory, and disk resources.
- Each computer needs to be maintained separately (for such operations as software upgrades and antivirus database updates).
- After a computer is shut down, the data customized by the user can be saved.
- The restoration upon shutdown function is not supported.
- The one-click restoration function is supported.

Principles of Full Copy

- A full copy computer is an independent computer created using the source computer template. In this mode, the created computer shares nothing with and is entirely separated from the source computer template, and will not be affected even if the source computer template is modified or deleted.

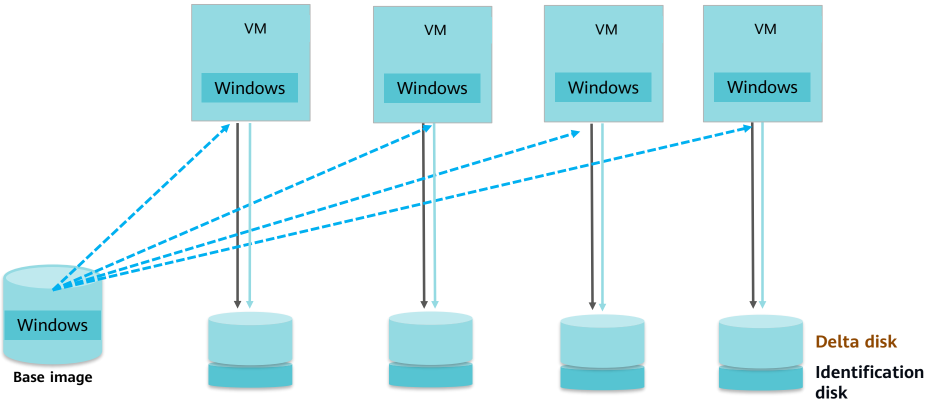
Characteristics of Full Copy

- Each full copy computer is an independent entity that enables users to save data changes, for example, software installation.
- However, the source computer template and each full copy computer use independent CPU, memory, and disk resources. You need to maintain software, for example, upgrade software or update the antivirus database, on each full copy computer.

QuickPrep VMs

- Principles
  - A QuickPrep VM is not encapsulated using Sysprep, but is renamed and added to the domain by applications in the VM.
  - There is no essential difference between full copy and QuickPrep.
- Advantages
  - The QuickPrep template is more efficient at VM provisioning than the full copy template.

A Linked Clone Desktop

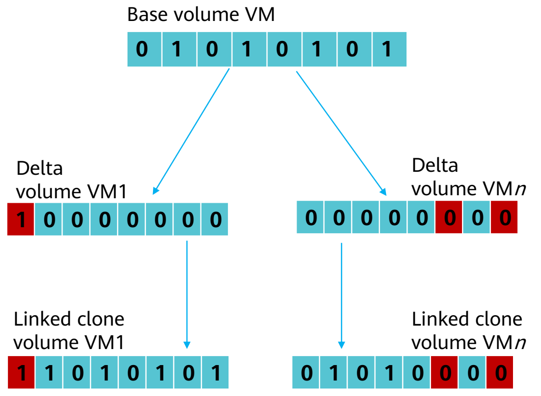


Higher management efficiency   Faster creation   Lower storage costs

Currently, linked clone is a mainstream desktop virtualization mode.

Principles of Linked Clone

- A linked clone computer is created using the source computer template. The computer can run only when the source computer template exists.
- Linked clone is a technology that maps a base volume and a delta volume to a linked clone volume for VMs. The linked clone base volume is read-only and is shared by multiple linked clone VMs.
- The linked clone delta volume can be read and written, whose storage is thin-provisioned. Each linked clone VM has a delta volume for storing differentiated data.



- The linked clone technology features fast creation and small storage usage, and is applicable to homogeneous users and highly standardized desktops.
- Because the base disk is shared by many desktops, it must offer high read performance.

Advantages of Linked Clone

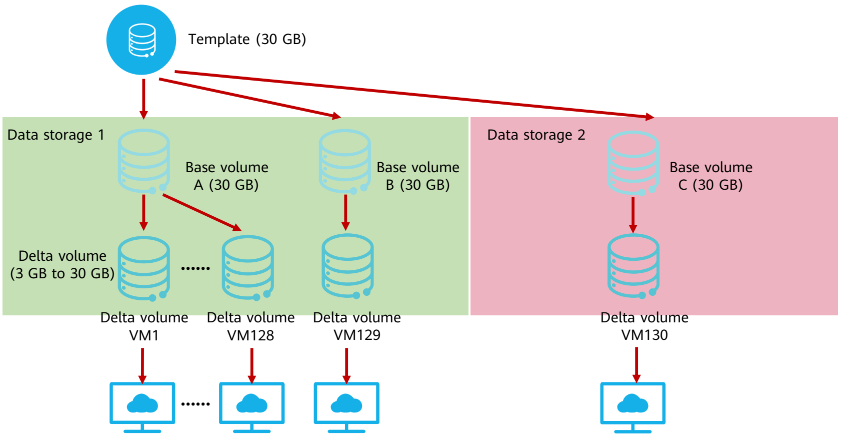
- Administrators upgrade multiple systems and install system patches and new software for linked clone VMs together.
- A shared base disk means no need to copy the system disk.
- The delta disks of the linked clone VMs store temporary user data, which can be automatically deleted when the VMs are stopped.
- Active Directory (AD) stores the personalized configurations and data of users.

- To update the base disk, the original linked clone template is cloned as a VM, and then this VM is started to update related systems. After that, this VM is converted to a template, and the function of updating VM group software is used. The O&M is simplified to ensure better IT system security and reliability.
- If users of linked clone desktops need to store customized configurations and data, configure profile redirection or folder redirection on the AD for these users. The redirection storage location can be a remote file server directory, a web disk, or the data disk of a linked clone VM. Customized configurations and data stored in remote file server directories or web disks can roam to the corresponding desktop to which the user logs in.

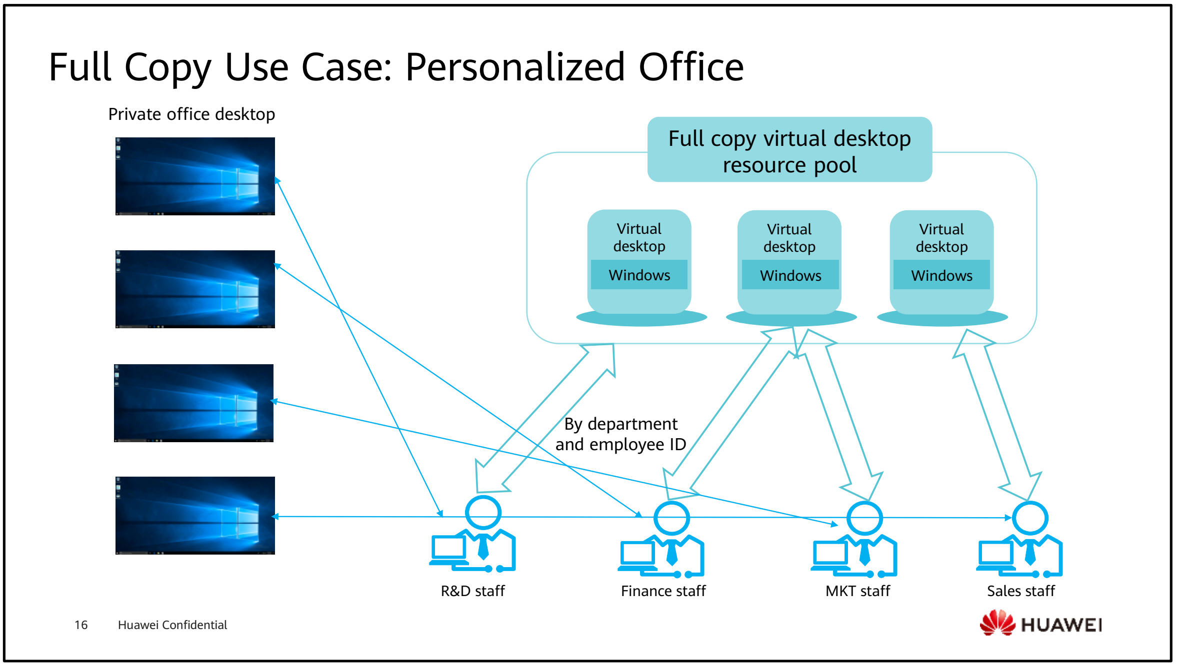
Benefits of Linked Clone

- Linked clone improves efficiency and saves costs.
  - VMs can be created in seconds, so overall provisioning is faster.
  - A large amount of storage space can be saved, lowering enterprise IT costs.
  - Unified system updates and patch installation for linked clone VMs make O&M more efficient and cost-effective.

Template, Base Volume, and Delta Volume

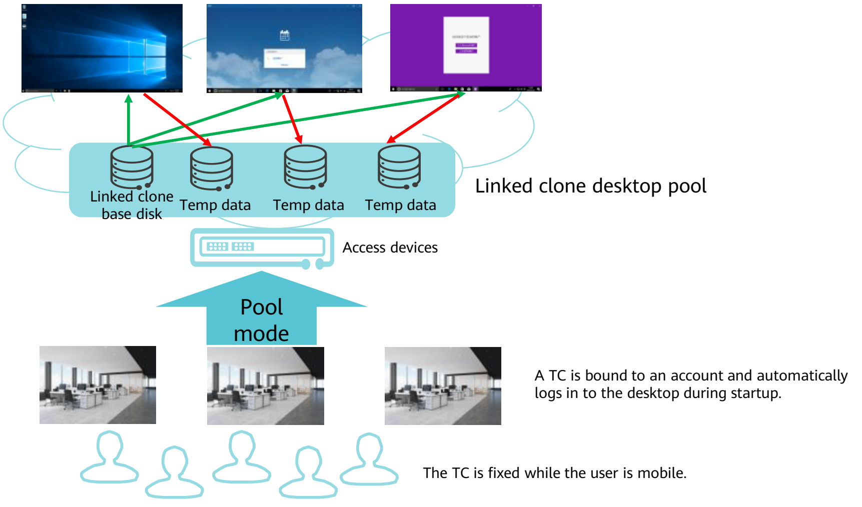


- As shown in the preceding figure, if the size of a linked clone template is 30 GB, when a linked clone VM is created on data storage 1, the template is automatically copied to generate a 30 GB base volume A, and then the automatic snapshot function is used to create a delta volume for each VM. When there are 128 delta volumes on the base volume A, the system automatically generates a base volume B in data storage 1 and creates delta volumes for other linked clone VMs. A maximum of 128 delta volumes can be created for each base volume to prevent high I/O pressure when all VMs are running.
- The delta disk created for each VM adopts thin provisioning. The initial size of each delta disk is nearly 0 GB. To store data, the estimated size of a delta disk is no less than 3 GB but not greater than that of a template. Generally, 5 GB, 10 GB, or 12 GB capacity is estimated for a delta disk based on application scenarios and restoration frequency of linked clone VMs.
- As shown in the preceding figure, the base disk and delta disk must be deployed on the same data storage. The template can be deployed on another data storage. Linked clone VMs can be created only on data storage that supports thin provisioning.



- In personalized OA scenarios, each employee from different departments may have different requirements on desktop settings, so they need customized desktops.
- Features of a full copy virtual desktop:
  - It is an independent computer that is created using a source computer (not joining a domain) template.
  - Users can save data changes (such as installed software) on computers.
  - Target computers have their own CPU, memory, and disk resources.
  - Each computer needs to be maintained separately (for such operations as software upgrades and antivirus database updates).
  - After a VM is shut down, users can save their customized data.
  - Restoration upon shutdown is not supported.
  - One-click restoration is supported.

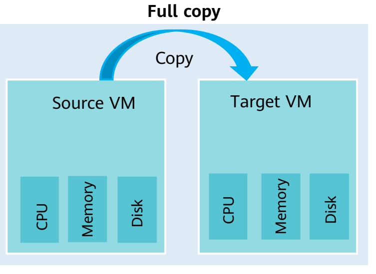
Linked Clone Use Case: Public Reading Room

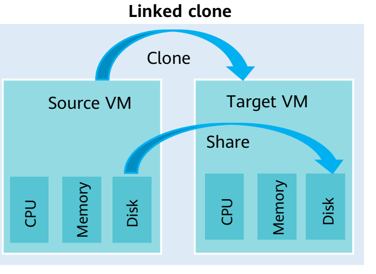


- In an electronic reading room, users only need to log in to and use VMs. The reading software has been contained in image files, and the service is simple. An electronic reading room has the following characteristics:
    - Users can access the Internet, but the viruses and Trojan on the network are difficult to prevent.
    - Users are not fixed, and VMs do not need to be frequently shut down.
    - USB flash drives must be supported.
    - Maintenance is simple.
- The electronic reading room has low storage requirements but faces security threats. Linked clone desktops are suitable for the electronic reading room. Linked clone VMs share a read-only base disk. The base disk is preinstalled with the required applications to prevent viruses or Trojan. When users log in to the linked clone VMs, temporary data generated during Internet access and web page browsing is stored on delta disks. If the delta disks are attacked by viruses and Trojan, you only need to restart the VMs to clear data on the delta disks. If VMs need to be upgraded or patches need to be installed on VMs, the administrator only needs to update the base disk.
- VMs can be assigned to multiple users dynamically for better resource reusability. Each TC is bound to a fixed VM account, and the TC can be logged in to once powered on. Users do not need to enter accounts or passwords when they log in.

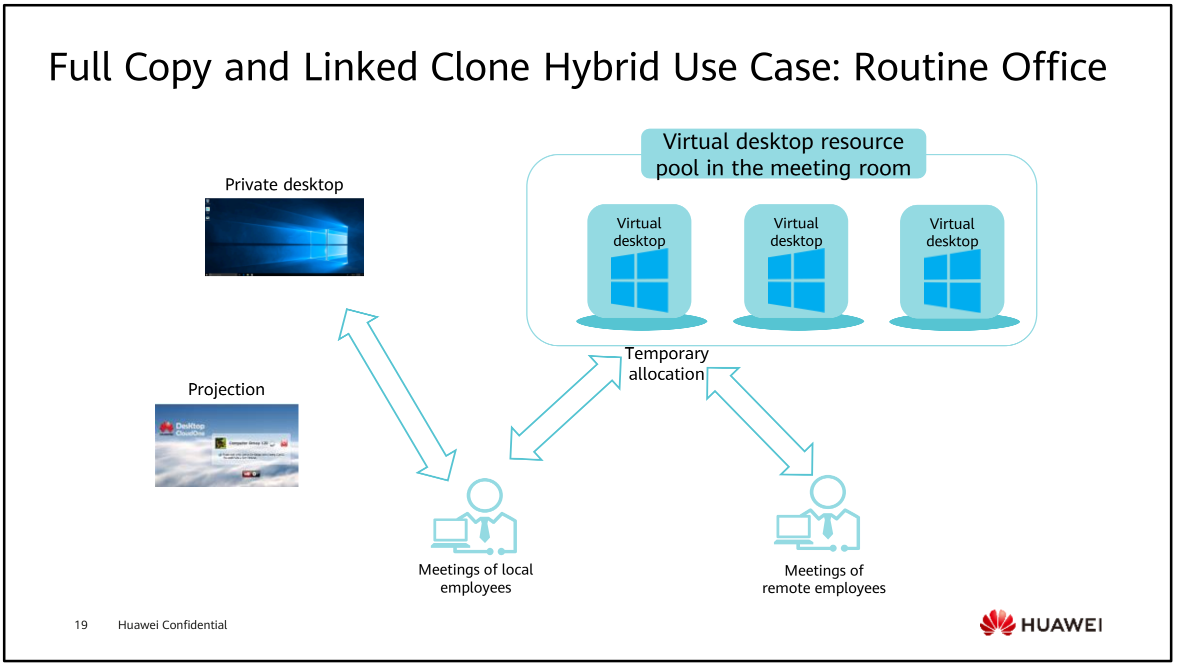
Full Copy vs Linked Clone (1)

- The major difference is in the system disk:
  - Multiple linked clone VMs share the same base disk. Each cloned VM has a delta disk to record write data to its system disk. Data includes temporary data, personalized configurations saved in C:\User, and temporary personalized applications saved in C:\Program Files. Together, the base disk and the delta disk constitute the system disk (drive C) of a linked clone VM.





- Administrators can forcibly reinitialize linked clone VMs and update applications for VMs in the linked clone VM group in a unified manner to update system base disks of linked clone VMs.

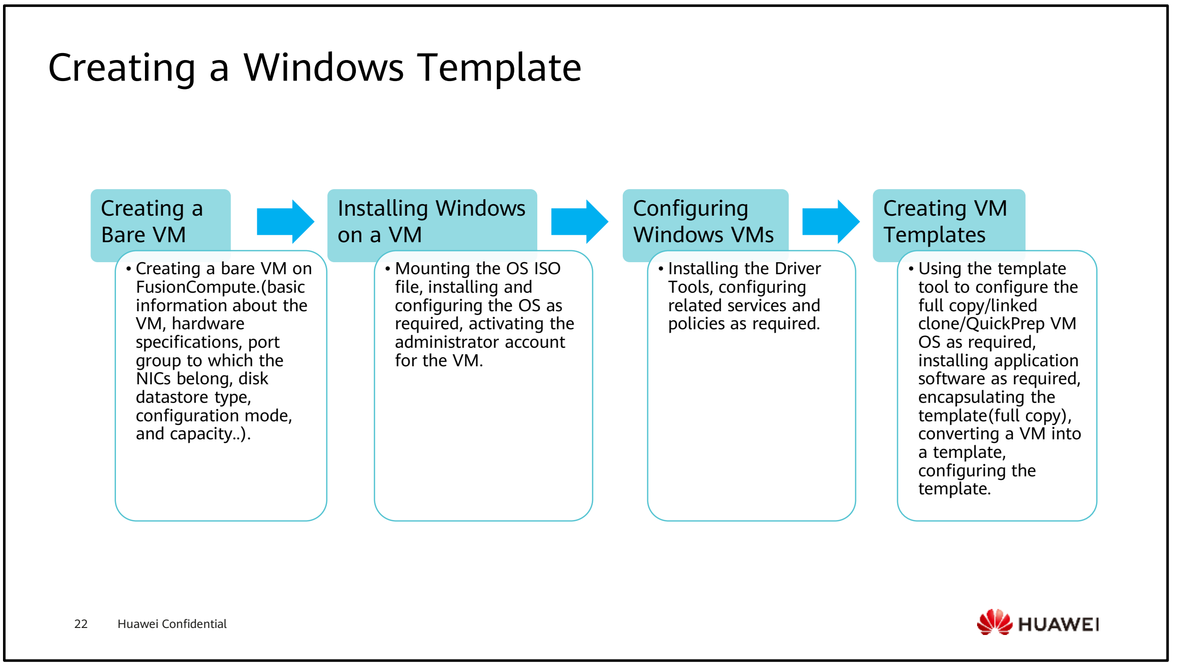


- Personal office desktop: full copy
- Meeting desktop: linked clone
- The meeting room desktop has the following characteristics:
- Applies to all users who use computer resources in meeting rooms.
- Application scenarios: pre-meeting shared document preparation, in-meeting document sharing and projection, and after-meeting local meeting material clearing.
- Scenario characteristics:
  - The application scenarios are limited, mainly material sharing and projection. Besides, the use duration is short, about 2 to 4 hours.
  - The local employees have their own desktops, and there is a physical distance between the office and meeting room.
  - Remote employees do not have private desktops. The desktops should not contain data of the previous user.
  - When local employees hold a meeting in a meeting room, they can log in to their own desktops through local TCs. After the meeting, the employees can log out of the desktops.
  - A virtual desktop resource pool is created to dynamically assign linked clone desktops to remote employees. To this end, the user group and virtual desktop resource pool of the meeting room must be bound. When a remote employee logs in to the desktop each time, the system randomly assigns a VM to the employee. After the employee logs out, the VM is reclaimed by the resource pool and the meeting data is cleared.

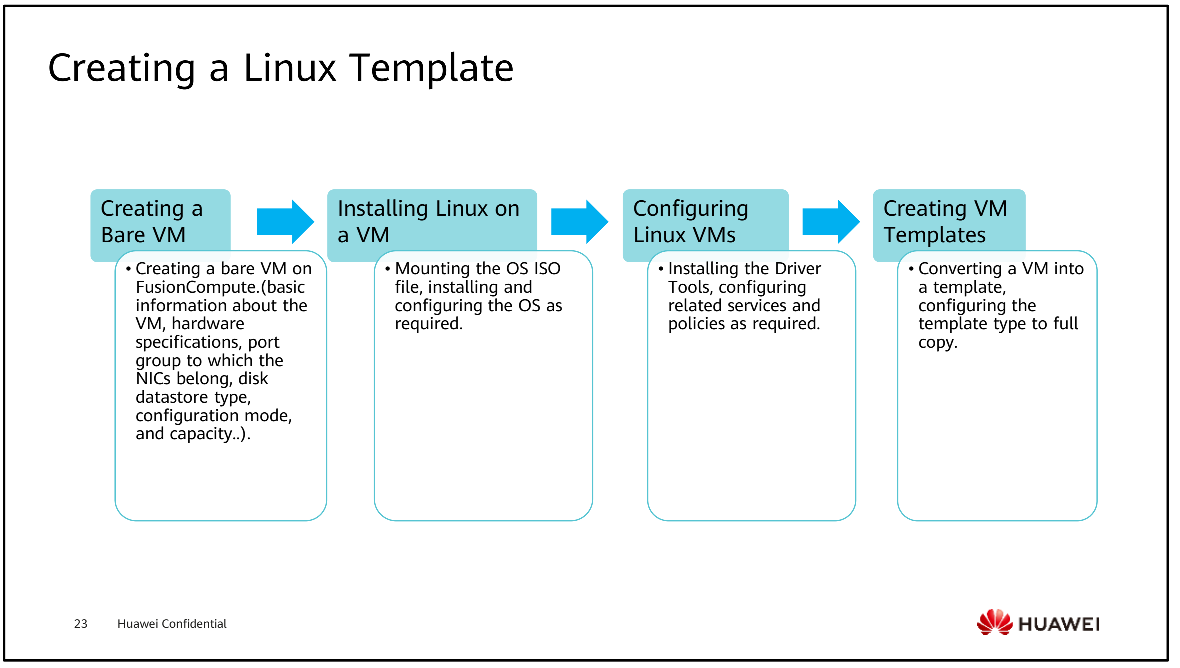
Comparison of Desktop VMs

Type	Provisioning Mode	Description	Provisioning Rate	Key Features of Desktop Components
Full copy	Full copy	Each VM has a system disk with independent storage space, repeated data results in storage wastage, VM creation is slow, and VMs lack unified update/restore.	Slow	Each VM is independent and can store personalized data.
	QuickPrep	Same as the above.	Medium	Each VM is independent and can store personalized data. VMs using the same template have the same SID.
Linked clone	Linked clone	Multiple VMs share a base disk but have an independent thin-provisioning delta disk, less storage space is used, VM creation is fast, and VMs have unified update/restore.	Fast	Multiple VMs share a system volume. VMs created using the same template have the same SID. VMs can be restored after shutdown but do not save personalized data.

Contents



- A local Windows user can log in to each Windows VM created using the image. For security purposes, you are advised to delete unnecessary local Windows users.
- Before using **Sysprep**, confirm that the IP address and the DNS server address can be automatically obtained.
- During the operation, if you are prompted to restart the VM, use the **Administrator** account to log in to the VM after the VM is restarted.
- If an exception occurs during the restart (restart fails), manually start the VM, mount the template tool ISO file again, and go to the template tool directory to reinstall the template tool.
- If **Configure user login** is not selected during the template creation, the VMs cannot be assigned to users in the **Users** group during quick desktop provisioning.
- Creating Linked Clone or QuickPrep VM Templates don’t need encapsulate the template. Before stopping the VM, confirm that the IP address and the DNS server address can be automatically obtained.



- During the operation, if you are prompted to restart the VM, use the **Administrator** account to log in to the VM after the VM is restarted.
- If an exception occurs during the restart (restart fails), manually start the VM, mount the template tool ISO file again, and go to the template tool directory to reinstall the template tool.
- VMs provisioned using this template can be provisioned only to domain A.
- During template creation, ensure that the VM can communicate with the AD server and parse the domain name of the AD server.
- If **Configure user login** is not selected during the template creation, the VMs cannot be assigned to users in the **Users** group during quick desktop provisioning.

System Encapsulation - Windows

- Definition
  - This records a system image to a virtual drive for system installation. Different from normal system installation using the Setup program, system encapsulation copies a complete system and installs it on another system disk.
- Advantages
  - The system installation time is greatly shortened (just 5 to 10 minutes).
  - It allows you to add your favorite applications to the system.

HUAWEI

- During the installation of the Windows OS, the Windows OS restarts and then the Windows UI is displayed to install the Windows components and configure the network, user, and CDKEY. This process takes about 10 minutes. System encapsulation includes the steps performed following the display of the Windows UI. In this way, when the system is started again, initial deployment such as component installation and network configuration is performed again.

System Encapsulation Tool - Sysprep

- Sysprep lets you:
  - Delete specific system data from Windows.
  - Configure entering of the audit mode for Windows on startup.
  - Configure entering of the **Welcome to Windows** page for Windows on startup.
  - Reset Windows product activation.

- Sysprep can remove all system-specific information from an installed Windows image, including the computer security identifier (SID), and then capture and install the Windows OS through organizations.
- You can install third-party applications and device drivers and test the functions of your computer in audit mode.
- Typically, computers are configured to after-startup entering of the **Welcome to Windows** page before being delivered to customers.
- Sysprep allows resetting Windows product activation up to three times.

Why Is Sysprep Necessary?

- The Microsoft operating system uses security identifiers (SIDs) to identify computers and users. Domain administrators assign machine SIDs and user account SIDs to computer accounts and user accounts respectively.
- If multiple PCs are cloned from a host or multiple VMs are cloned from a VM template, the clones share the same SID. As a result, the PCs or VMs cannot be identified or added to the domain. In the same LAN, computers or accounts with the same SID may encounter problems with permissions and security.

- Therefore, when creating a full copy template, you need to perform the Sysprep operation that deleting all system identification information, such as the computer security identifier (SID), from the installed Windows image to avoid the preceding problems.

Contents

Basic Concepts Introduction

Concept	Description
Computer	A computer provides desktop resources and can be assigned to different types of end users. VMs mentioned in this course can be regarded as computers.
Bare VM	A bare VM created on FusionCompute can be used to create various types of computer templates.
Template	After a bare VM is configured and optimized or equipped with software, the VM can be converted into a template. The template can be used to create computers for users.
Computer group	Computers can be grouped to simplify computer management.
Desktop group	A desktop group is a group of computers assigned to domain users or domain user groups.
Domain user	A domain account is the only credential for a user to log in to a desktop and thereby needs to be created before desktop provisioning.
Domain user group	Domain users can be grouped to simplify user management.
User	Users are those who can access FusionAccess.
User group	Users can be grouped to simplify user management.
Private	A private desktop group is composed of full copy computers.
Static pool	The system randomly assigns a computer in a desktop group to a user when the user logs in for the first time. The user will always use this computer to access the desktop. Full copy computers and linked clone computers are supported.
Dynamic pool	Computers in a desktop group are randomly assigned to users and no fixed binding relationships exist. Each time a user logs in to a computer through the Web interface (WI), an idle computer is dynamically selected from the pool and assigned to the user. Full copy computers and linked clone computers are supported.

- Desktop groups are classified into private, static and dynamic pools.
- Each computer in a private desktop group can be assigned to one or multiple users.
  - Assign a computer to a user: a computer can be used by only one domain user.
  - Assign a computer to multiple users: a computer can be used by multiple domain users, but multiple users cannot use the computer at the same time.
- Desktop groups are classified into dynamic-pool desktop groups and static-pool desktop groups. Dynamic pools and static pools are called pooling mode. **Assignment Type** for computers in pooling mode is **Assign computers to a desktop group**.

Quick Provisioning Overview

- FusionAccess simplifies provisioning operations with a wizard, which enables administrators to provision virtual desktops in batches.
- Quick provision is based on tasks. Administrators only need to create tasks as prompted. The FusionAccess system performs subsequent operations in the background without manual intervention.
- Administrators can monitor task progress in the task center.

Quickly Provisioning a Computer

Creating a computer

- Configuring a computer group, a template, CPU and Memory (MB), a disk, NIC information, domain name, the number of computers, a naming rule for computers and advanced information as required.

Assigning computers

- Configuring a desktop group, assignment type and assigning Computer, including assignment type, the number of assigned computers, user(group) and user permissions.

Confirming the information

- Check the configuration of the computer to be provisioned. If the configuration is correct, click OK.

Finishing the procedure

- It takes about 20 minutes to provision the computer. After the quick provisioning task is complete, a new computer is created. You can view and manage the computer on the Resources > Desktops > Computers page.

Parameters for Creating a Computer (1)

- Computer group: to select existing computer group or creating new computer group.
- Computer group name: to select a pre-defined name or creating a new name.
- Computer type shown below:
  - Full Copy
  - Linked Clone
  - QuickPrep

- When creating a computer, you need to add the computer to the specified computer group.
- Full copy: each VM in the computer group is assigned a system disk, and the provisioning mode is Full Copy or QuickPrep.
- Linked clone: multiple VMs in a computer group share a system volume, which features fast creation and software update. The provisioning mode is linked clone.

Parameters For Creating a Computer (2)

- Configure a template
  - Site: sum of computing, storage, and network resources in the system.
  - Cluster: logically divides computing, storage, and network resources at a site.
  - Host (optional): to filter data stores by host, ensure that the new computer can run on the host.
  - Template: to select the desired template of defined type.
  - CPU and Memory (MB): retain the default values of or set new values.
  - Disk: to select the data storage and configuration mode as required, including system disk and data disk.
  - NIC: to select the service-plane port group (security group) and set the IP address obtaining mode as required.

- The total number of data disks cannot exceed 10 and adding data disks will prolong the provisioning time. If too much data is stored in the template, you are advised to specify the data store of the system disk, when creating linked clones, to improve the provisioning efficiency. When a linked clone is being provisioned, the data disk in the template will be formatted.
- How IP Address Obtained
  - The system automatically assigns IP addresses to computers.
  - The administrator specifies the start IP address for a computer. Only the first NIC supports static IP addresses.
- For a linked clone template, the **Configuration Mode** of the system disk must be set to **Thin provisioning**.

Parameters for Creating a Computer (3)

- Domain name: the domain name of a QuickPrep or linked clone template must be the same as the domain name of the domain to which the VM template is added during template creation.
- The number of computers: before creating computers in batches, you can provision a few (less than five recommended) computers to ensure that the computers can be successfully provisioned. You can create a maximum of 100 computers at a time.
- A naming rule for computers: to select an existing naming rule or create a new naming rule.
- Advanced information: retain the default values or configure the parameters as prompted.

- A maximum of 50 naming rules can be created.
- Whether a computer name contains the domain account used to log in to the computer.
  - The names of computers included in static or dynamic pools cannot contain any domain account.
  - When setting a naming rule for linked clone computers, select No.

Parameters for Assigning Computers (1)

- HDC: to select preconfigured HDCs as required.
- Desktop group: to select an existing desktop group or create a new desktop group.
- Desktop group name: automatically associates the existing desktop group name or create a new desktop group name.
- Desktop group type: to select Private, Static Pool, or Dynamic Pool as required.

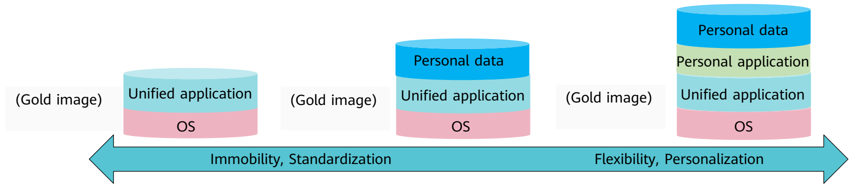
- When assigning a computer, you need to add the computer to the specified desktop group.
- A desktop group can be assigned with computers running only one operating system. For example, if a desktop group has been assigned with Windows computers, the desktop group cannot be assigned with Linux computers.
- If the AD domain name is included in the naming rule, the desktop group type can only be set to Private.

Parameters for Assigning Computers (2)

- Assignment type: to select an assignment type based on the desktop group type.
- Assign computer: the number of computers to be assigned must be less than or equal to the number of created computers.
  - Add user (group): to add an existing domain user or create a domain user.
  - Set permission groups: to select administrator or users.

- You can manually enter the name of an existing user (group). The format is LiteAS user (group) name, third synchronize user (group) name, or AD user (group) name@AD.
- When Assignment Type is set to Single User, only one user name can be entered. If Assignment Type is set to Static Multi-User, you can enter multiple user names and use commas (,) to separate multiple user names.
- Set permission groups:
  - administrators: indicates the administrator group. Group users have system administrator permissions, that is, full control permissions on a computer. They can perform all management tasks, including managing all users, on the computer.
  - users: indicates the basic user group. Group users have basic operation permissions on a computer, for example, running applications. They cannot change the OS settings or data of other users, or shut down a server computer.

Multiple desktop deployment modes to match different service scenarios



Scenario Category	Scenario Description	deployment model
Personalized program and data	●Users have personalized application installation requirements. ●Users have personal data storage requirements. ●Typical scenarios: daily office、R&D office	● 1:1 private desktop (full copy desktop)
No personalized program but personalized data	●Users do not have personalized application installation requirements. ●Users have personal data storage requirements. ●Typical scenario: call center	● M:N pooled desktops (linked clone desktops) ● Personal data and configuration: NAS web disks and profile roaming are used to store personal data.
No personalized program and data	●Users do not have personalized application installation requirements. ●Users do not need to store personal data. ●Typical scenarios: meeting rooms、training classrooms	● M:N pooled desktops (linked clone desktops) + automatic restoration upon shutdown

- A gold image is a pre-configured image file that contains a complete copy of a system or application. This image file can be used to quickly deploy multiple systems or applications with the same configuration.

Differences Between Full Copy, Linked Clone, and QuickPrep

Differences	Full Copy	Linked Clone	QuickPrep
Template making	No domain needs to be added. Encapsulation is required.	Domains need to be added. Encapsulation is not required.	Domains need to be added. Encapsulation is not required.
Disk Components	Independent system disk + data disk(optional)	Linked clone volume (formed by the logical combination of the base volume (shared) and delta volume) + Data disk (optional)	Independent system disk + data disk(optional)
Desktop group type	Private	Static and Dynamic Pools	Private
Provisioning speed	Slow	Fast	Medium
Provisioning procedure	Decapsulation required	No decapsulation required	No decapsulation required
application scenario	High-security desktop, high-performance graphics processing, Personalized data or application scenarios are available.	Personalized data but no personalized applications are available, or No personalized data, no personalized application scenario	Used in test
Updates and upgrades	Perform operations on each VM.	Update the template and use the template to update VMs in batches	Perform operations on each VM.
Restore function	Power-off restoration is not supported, but one-click restoration is supported.	Automatic power-off restoration	Power-off restoration and one-click restoration are not supported.

Quiz

1. Which of the following files is required when creating a desktop template?
   A. FusionAccess_Linux_Installer_*xxxxx*.iso
   B. FusionAccess_LinuxDesktop_*xxxxx*.iso
   C. FusionAccess_WindowsDesktop_Installer_*xxxxx*.iso
   D. FusionAccess_WindowsDesktop_*xxxxx*.iso
2. VM template creation is not required if virtual desktops are provisioned in quick provision mode.
   A. True
   B. False

- Answers:
  - C
  - B

Summary

- This course described the concepts, principles, and applications of FusionAccess full copy and linked clone, differences between them, and how to create full copy and linked clone templates and provision virtual desktops.
- Subsequent courses introduce operations such as policy management and service adjustment after virtual desktop provisioning.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Acronyms and Abbreviations

SID: Security Identifiers

VNC: Virtual Network Console

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

FusionAccess: Features and Management

HUAWEI

Foreword

- Huawei FusionAccess lets you manage virtual desktops by customizable policies and service adjustment. In case of a fault, an alarm is generated to help you resolve the fault quickly.
- This course describes the management and routine O&M of Huawei FusionAccess virtual desktop features.

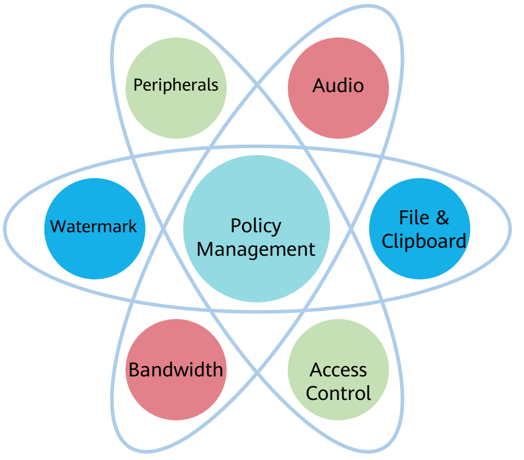
Objectives

- On completion of this course, you will be able to:
  - Learn about desktop policy management in FusionAccess.
  - Master FusionAccess service adjustment operations.
  - Understand the routine O&M of the FusionAccess.

Contents

Policy Management

- Create application policies for all computers in a computer group, a computer, or computers of a user as needed in different scenarios.



- You can create policies in terms of peripherals, audio, multimedia, client, display, file and clipboard, access control, session, bandwidth, virtual channel, watermark, keyboard and mouse, audio and video bypass, personalized data management, and customization.

Policy Classification

Classification	Description
Protocol Policies	The protocol policy provides customized configuration to meet users basic OA requirements and special scenarios requirements. It can be done in many ways. (e.g. peripherals, audio, client, display, file and clipboard, access control, watermark, keyboard and mouse) Customization policies.
Access Control Policies	There are access time control policies and gateway authentication policies, the access time control function is used to forbid specified objects from accessing computers in specified time segments. Ensure that the time is consistent on the two components ITA and HDC. Their time zones must be the same too.
Terminal and User Binding Policies	Configure user binding. After a user is bound to a terminal, the user can use only the bound terminal to log in, ensuring information security.
Terminal and Desktop Binding Policies	The system supports configuring terminal and desktop binding. After the binding relationship is configured, the bound desktop can be logging in using only the bound terminal.

- Access control in the protocol policy refers to IP access control. This function allows users to access the cloud desktop only from clients in the specified IP address segment. This policy takes effect after you choose System > System Configuration > Desktop Components and configure a service access gateway on the WI page. If this policy is not configured, all client IP addresses are allowed to access the by default.
- The rest of this course focuses on Protocol Policy.

Protocol policy creation mode

Creation Mode	Description
Create Using a Template	Create a policy group using an existing policy group template, with the same configurations as those of the template by default.
New Policy Group	Use the default blank template to create a policy group.
Import from the Policy Group	If a policy group has been created, you can import a policy from an existing policy group. The configurations are the same as those of the policy by default.

HUAWEI

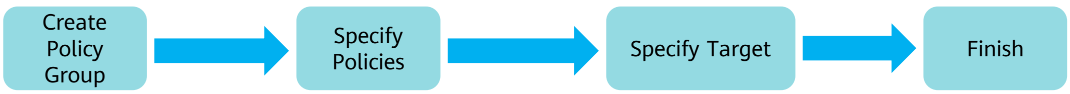
- If you select **Create Using a Template**, the administrator can select an existing policy template or create a template by adding a user-defined template.

Default Policy Template

Classification	Description
Security Scenario	In security scenarios, HDP is used to prevent data from being sent to personal storage devices, ensuring that data assets are stored only in enterprise data centers.
Game Scenario	In gaming scenarios, the cursor tracking and image display are optimized, ensuring smoothness and improving gaming experience even in low bandwidth conditions.
Graphics Processing Scenario	In graphics processing scenarios, the display frame rate is adjusted to improve the image display quality and the cursor tracking mode is adjusting to reducing the spacing between the cursor and the image and minimize visual differences.
Video Editing Scenario	In video editing scenarios, video acceleration is used to optimize video playback quality. The cursor closely tracks user operations, improving user experience.

Process of creating a protocol policy

- On the FusionAccess **Home** page, choose **Policy Management**. The **Protocol Policies** page is displayed.



Specify Policies

- On the **Specify Policies** page, set application policies for the computer based on user requirements.
- Policies include **Peripherals, Audio, Multimedia, Client, Display, File&Clipboard, Access Control, Session, Bandwidth, Virtual Channel, Watermark, Keyboard&Mouse, Audio and Video Bypass, Personalized Data Mgmt,** and **Custom**.

Specify Target-Target Type

- Desktop Group
- Computer
- VIP Desktop
- User
- User Group
- OU
- Client IP Address
- WI

- If the name of the selected application object contains the **Desktop Group** object type, the policy will be applied to all computers in the related desktop group.
- When the target type is **Client IP Address**, please enter a valid IP address or IP address and subnet mask.
- When the target type is **Desktop Group/Computer/VIP Desktop/WI**, it supports searching all data, and also supports using the prefix of target name for fuzzy search.
- When the target type is **User/User Group/OU**, only target names can be used for fuzzy search.

Scenarios

- Policy for audio scenarios
  - For daily work or conferences that do not allow audio recording and playback, disable **Audio Redirection**.
  - Set **Play Volume** only in education scenarios, such as online classrooms that need a set volume.
- Policy for display scenarios
  - For desktop environments that require high definition, choose **Display** > **Display Policy Grade** to expand advanced settings and modify parameters such as **Bandwidth**, **Lossy Compression Recognition Threshold**, and **Lossy Compression Quality**.
  - Server decoding: playback of local and network videos. Multimedia redirection: local video playback. Flash redirection: network video playback.

Contents

Modifying Computer Specifications

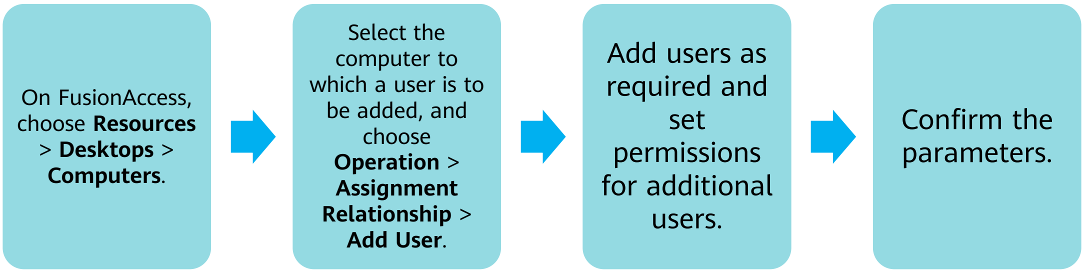
- In office scenarios, if the CPU or memory of a computer is insufficient, the normal office is affected. Administrators can modify the computer specifications based on the actual situation to meet user requirements.

On FusionAccess, choose **Resources** > **Desktops** > **Computers**. → Select the computer to be modified and choose **Operation** > **Change** > **Modify Computer**. → The Modify Computer page is displayed. Modify the computer parameters as required. → Confirm the parameters (restart the computer as required for the modification to take effect).

- After the CPU and memory specifications of a running computer are modified, the modification takes effect only after the computer is restarted. The administrator restarts the computer or the administrator informs the end user to restart the computer.
- For computers in other states, the modification will take effect upon startup.

Adding a Computer Domain User

- In some specific office scenarios, multiple employees share one computer. If a new employee needs to use the computer, the administrator can add a domain user to the computer so that the new employee has the permission to use the computer. This scenario applies only to computers whose assignment type is **Assign a computer to multiple users**.



- When **Assignment Type** is set to **Assign a Computer to Multiple Users**:
  - If user A has logged in to a computer, user B cannot log in to the computer.
  - If user A disconnects from a computer without logging out, user B can log in to the computer and user A will be forcibly logged out of the computer at that time.
  - Multiple users share the same computer. The data stored on the drives of the computer by one user can be accessed by other users. Therefore, do not store sensitive personal data on the computer.
  - To ensure all users in user group A can log in to the pool desktop that is assigned to this group, all these users must directly belong to user group A.
    - For example, if user A belongs to department A and department A belongs to department C, user A can directly log in to the pool desktop if it is assigned to department A, but cannot log in to the pool desktop if it is allocated to department C.

Adding a Computer

- Because different departments have different service requirements, computers in each department are managed by group. This slide describes how to add a computer to a department's computer group for a new employee. This operation includes adding a computer to a computer group and assigning the computer to a desktop group.

On FusionAccess, choose **Resources** > **Desktops** > **Computer Groups**.

→

On the right of the computer group to which a computer will be added, choose **Operation** > **Add Computer**.

→

Set related parameters as required. (site, cluster, host, template, CPU, memory, disk, NIC, quantity, etc.)

→

On FusionAccess, choose **Resources** > **Desktops** > **Desktop Groups**. select the desktop group to be assigned, configure basic information about the desktop group, and assign the computer.

- Adding data disks will prolong the provisioning time.

Upgrading a Common Desktop to a VIP Desktop

- In a common office scenario, all computers request resources at the same priority. In specific scenarios, some virtual desktops have higher priorities for resource supply. In this case, you can upgrade these common desktops to VIP desktops so that users of these virtual desktops can be provided with preferential CPU and memory resource supply, real-time computer status monitoring, and better desktop experience. Administrators can flexibly upgrade common desktops to VIP desktops based on actual demands.

On FusionAccess, choose **Resources** > **Desktops** > **Computers**.

→

select one or more computers that have been assigned and need to be upgraded to VIP desktops. Choose **Operation** > **Set** > **Upgrade to VIP Desktop**.

→

In the displayed Confirm dialog box, click **OK**.

→

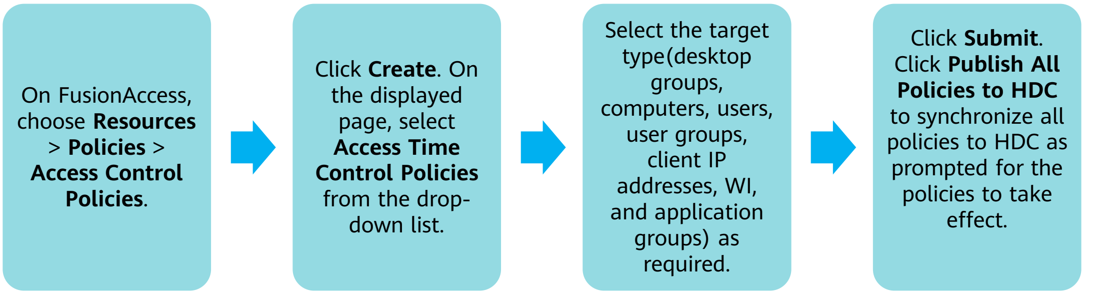
In the Prompt dialog box, click **OK**.

The computer automatically restarts. After the restart, the computer name is displayed in yellow.

- During the operation, the user computer needs to restart. The user computer is unavailable during the period of time.
- Retain default values for VIP desktop resource assurance and real-time monitoring policies for all VIP users.

Configuring User Access Control Policies

- In most cases, no restrictions are required to control user access. When you need to restrict access to VMs for protecting information within the VMs, configure access control policies.
- The process of Access time control is as follows:



- User access control policies include:
  - Access time control: Set multiple time periods and specify objects that are not allowed to access VMs during these periods.
  - Gateway authentication policy: Enable access control if you need to establish encrypted connections between clients and the server using the Chinese cryptographic algorithm.
  - Terminal and user binding: After the binding relationship between a user and a terminal is configured, the user can log in to the computer only through the bound device. The user cannot access the computer through other devices. This ensures the security of sensitive information on the computer. The administrators can group users or TCs for batch binding, reducing workloads.
  - Terminal and desktop binding: Once a computer is bound to a terminal, it can be logged in using only this terminal.

Unassigning a Computer and Restoring Assignment (1)

- When a user resigns, transfers, or changes in the work scope, the binding relationship between the computer and the user (group) needs to be changed accordingly. The administrator can unassign or restore the binding relationship based on the actual situation.

On FusionAccess, choose **Resources** > **Desktops** > **Computers**.

→ Select one or more computers to be unassigned and choose **Operation** > **Assignment Relationship** > **Detach**.

→ In the **Confirm** dialog box, click **OK**. In the **Unassigned List** dialog box, click **OK**.

→ Check the operation result in the computer list. If **Assignment Status** is **Unassigned**, the computer is successfully unassigned.

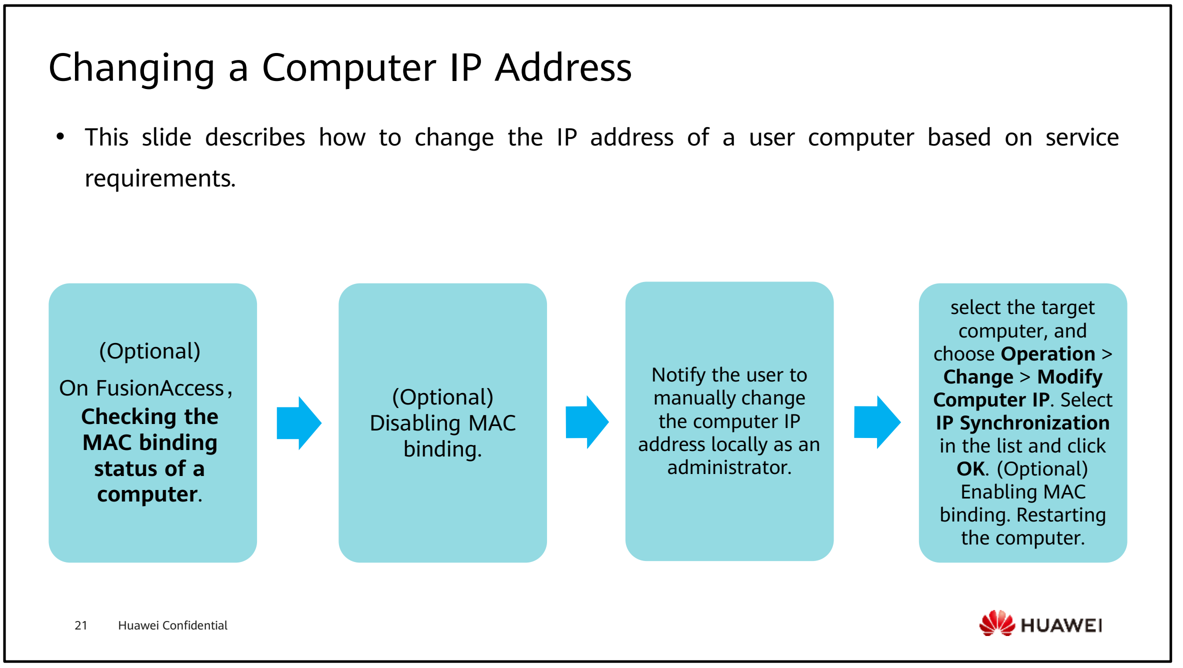
- The computer whose **Assignment Type** is **Assign a computer to a user** is automatically stopped after being unassigned.
- The computer whose **Assignment Type** is **Assign a computer to multiple users** or **Assign computers to a desktop group** cannot be assigned again after being unassigned.

Unassigning a Computer and Restoring Assignment (2)

- When a user resigns, transfers, or changes in the work scope, the binding relationship between the computer and the user (group) needs to be changed accordingly. The administrator can unassign or restore the binding relationship based on the actual situation.

1. On FusionAccess, choose **Resources** > **Desktops** > **Computers**.
2. Select the computer and choose **Operation** > **Assignment Relationship** > **Restore Attachment**.
3. In the **Confirm** dialog box, click **OK**. In the **Restore Allocated List** dialog box, click **OK**.
4. Choose **System** > **Tasks and Logs** > **Task Tracing**. Views the task execution status. The task is executed successfully when its status changes to **Completed**, **all jobs succeeded**.

- After a computer whose **Assignment Type** is **Assign a computer to a user** is unassigned, it can be assigned only to the original user and the user group permissions remain unchanged.
- After the unassigned computer is assigned and started, the computer icon on the WI turns on. The computer can be logged in 3 minutes later.



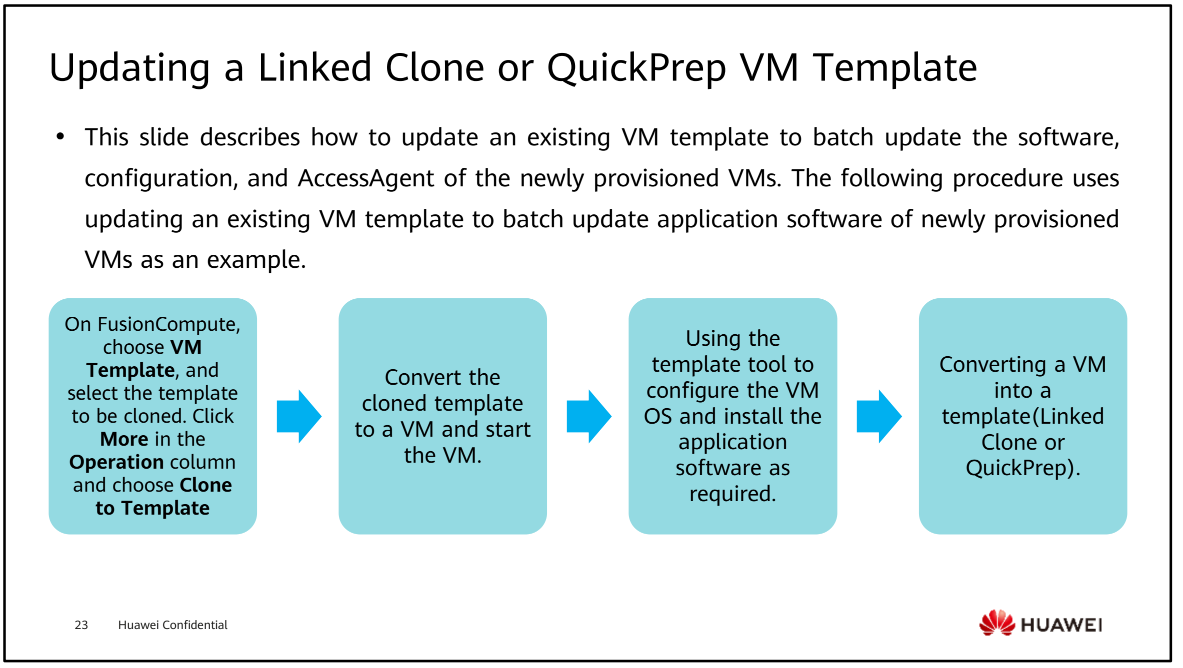
- The value of **How IP Address Obtained** is **DHCP** and that of **MAC Binding** is **Disabled**.
- When **Running Status** of the computer is **Migrating** or **Recovering**, MAC binding or unbinding is not allowed.
- IP synchronization can be performed for computers that are in the **Running** state.
- Restart the computer. Otherwise, the computer cannot be connected.

Updating a Full Copy VM Template

- This slide describes how to update an existing VM template to batch update the software, configuration, and AccessAgent of the newly provisioned VMs. The following procedure uses updating an existing VM template to batch update application software of newly provisioned VMs as an example.

On FusionCompute, choose **Resource Pools** > **VM Template**, and select the template to be converted. → Install application software on VMs as required. → Create a VM template (Full Copy) to complete the VM reconstruction. → Converting a VM to a template. (On the FusionAccess Windows Installer page, select Update Template.)

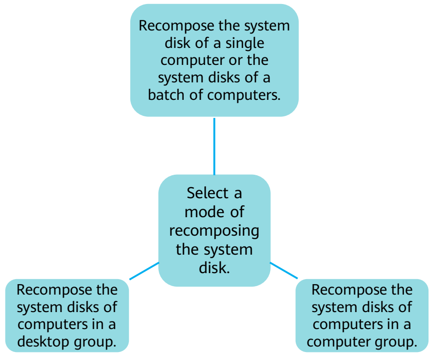
- This course takes updating the Windows operating system template as an example.



- After updating a linked clone template, you can delete the VMs and provision new VMs or recompose the system disk of the existing VMs by referring to Recomposing a System Disk.
- Deleting and provisioning VMs affect live network services. You need to make preparations in advance to ensure proper service running.

Recomposing a System Disk

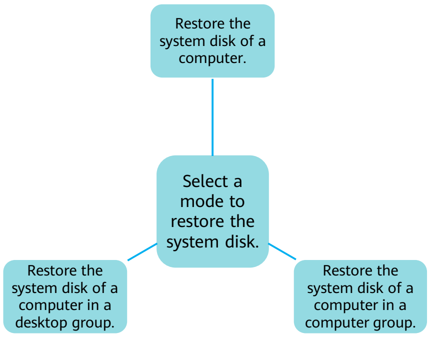
- This slide describes how to recompose the system disk of a computer or the system disks of all computers in a computer group using a template installed with office software of the latest version.



- The OS of the selected template is the same as that of the computer whose system disk is to be recomposed.
- Notify users to back up the system disk before recomposing it because only data on data disks of linked clone computers is retained and data on the system disk, such as **Desktop** and **Favorites**, will be lost after the recomposition. For a full copy computer, the original system disk can be retained and repurposed as a data disk.

Restoring a System Disk

- This slide describes how to restore the system disk of a computer without affecting data disks.



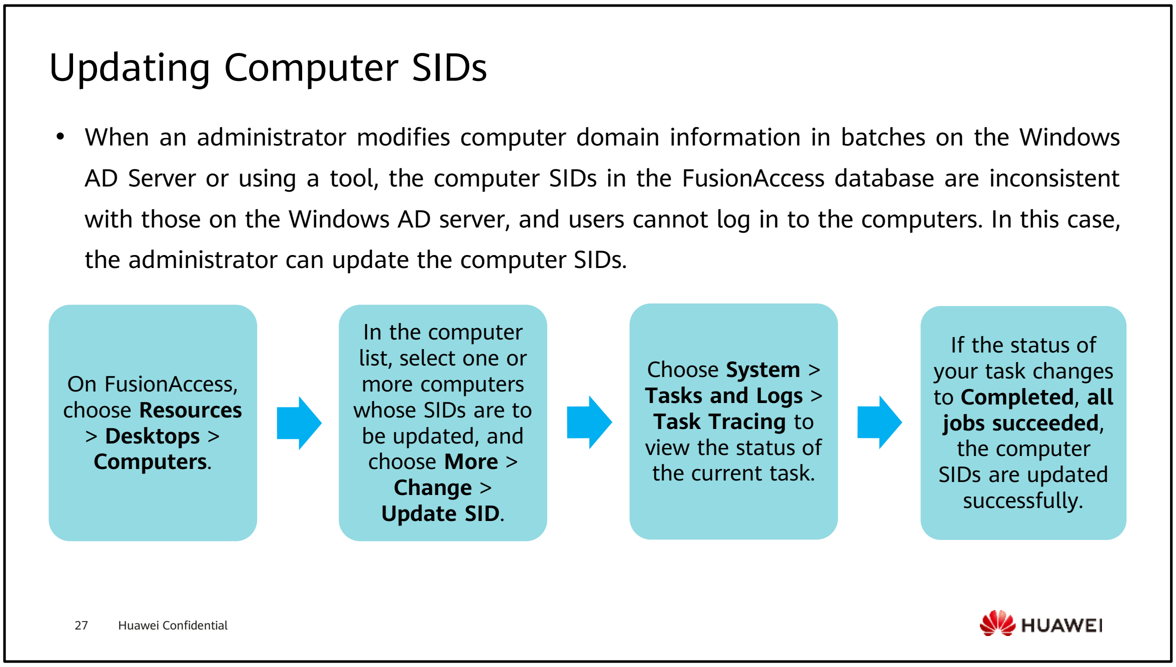
- Notify the user to back up the system disk before restoring it because only data on data disks of linked clone computers is retained and data on the system disk (such as the desktop and Favorites) will be lost after the restoration. For a full copy computer, the original system disk can be retained and repurposed as a data disk.
- The system disks of multiple computers can be batch restored only when the computers are of the same assignment type and created using the same computer template.

Setting Self-Service Backup

- The system administrator can enable the self-service backup function on end users' computers so that users can perform self-service desktop backup management on the WI or UNS, including backup and restoration of system disks and data disks that support snapshots on dedicated desktops.

1. On FusionAccess, choose **Resources** > **Desktops** > **Computers**.
2. In the computer list, select the desired computer, and choose **Operation** > **Change** > **Set User Self-service Backup**.
3. Enable **Set User Self-service Backup**.
4. Log in to the VM. Check whether **Back Up** and **Restore** exist.

- Prerequisites:
  - Assignment Status of the computer is Assigned.
  - Desktop types: desktops in 1:1 assignment mode in dedicated desktop groups and desktops that have been bound to users' in static pool desktop groups.
- FusionCompute supports the following data storage types: FusionStorage, SAN storage, NAS storage, and local disks.
- FusionCompute does not support the following disk types: shared disks, independent disks, non-persistent disks, and system disks of linked clone computers.
- Back Up: Only one piece of data can be backed up. If you back up the data again, the previous backup data will be overwritten.
- Restore: Data within the range you specified will be restored to the last backup time. Exercise caution when performing this operation.



- Prerequisites:
  - A full copy computer template is available.
  - Computers running the Windows have been connected to the Windows AD.
- The old and new SIDs of computers can be viewed.
- If computers are recomposing system disks or restoring system tasks, computer SIDs will fail to be updated.

Contents

Overview

- In the FusionAccess desktop products, the system management and maintenance operations include the following:
  - On FusionCompute Web Client, create infrastructure VMs and maintain and manage resource pools and system VMs.
  - On FusionAccess Web Client, manage FusionAccess accounts and user VMs, configure peripheral redirection policies, perform alarm management and scheduled task management, and view statistics.
  - On FusionAccess infrastructure VMs, perform account management, password management, license management, patch management, configuration, and backup and restoration of the maintenance system.

- For details about routine maintenance and management of FusionCompute, see the FusionCompute product documentation of the corresponding version.

FusionAccess Daily Maintenance Tasks (1)

Maintenance Item	Scenario	Maintenance Task
Component status monitoring	Monitor component status to quickly detect system exceptions.	Check the status of each component.
System alarm monitoring	Monitor FusionAccess alarms to quickly detect system exceptions.	Handle critical alarms immediately according to the alarm help. Handle non-critical alarms once a week according to the alarm help.
VIP desktop alarm monitoring	Promptly rectify faults for computers of VIP users.	Note: On FusionAccess Web Client, choose **Monitoring** > **VIP Desktop Alarms** > **VIP Desktop Policies** to configure monitoring items for VIP desktops. Regularly check VIP desktop alarms. Configure email notification to handle VIP desktop alarms in real time. Note: On FusionAccess Web Client, choose **Monitoring** > **Alarms** > **Email Notification** to configure them.

- VIP desktop policies
  - Resource assurance policy
    - CPU assurance priority
    - Memory assurance priority
  - Real-time monitoring policy
    - The computer registration status is abnormal. (That is, the computer is running but is not registered. In this case, users cannot log in to the desktop properly.)
    - The CPU usage exceeds 80%.
    - The system disk usage exceeds 80%.
    - The memory usage exceeds 80%.
    - The computer is shut down.

FusionAccess Daily Maintenance Tasks (2)

Maintenance Item	Scenario	Maintenance Task
Computer status monitoring	Monitor the operating status, login status, assignment status, performance consumption, and registration failures of user computers to detect and handle potential risks of the system early.	Collect computer status statistics. Collect computer performance statistics. Collect the number of abnormal computer registrations.
Gateway status monitoring	Routinely monitor whether CPU, memory, and traffic resources of a gateway match user resource consumption to identify irregular users immediately, such as high bandwidth consumers.	Monitor basic gateway information: gateway status. Monitor user connection information: the status of resources consumed by active users.

FusionAccess Weekly Maintenance Tasks

Maintenance Item	Scenario	Maintenance Task
User VM restart **NOTE:** It is recommended that users restart VMs by themselves.	Memory and process resource usage is high if the Windows OS runs for a long time. To ensure proper system running, it is recommended that user VMs restart once every week.	Restart user VMs every three to five days.
System backup check	Periodically check the backup function and backup data availability of the system to ensure that backup data is available when a system exception occurs.	Check whether backup data exists based on backup policies. If no, rectify the fault immediately.

Forbidden operations

Category		Risk
Service operations	Delete virtual desktops on FusionCompute.	Users' virtual desktops will be unavailable.
	Deploy the Dynamic Host Configuration Protocol (DHCP) servers or domain name servers (DNSs) in the desktop cloud.	The DHCP and DNS servers conflict with the DHCP and DNS services running on FusionAccess, resulting in service failures.

- Avoid the operations listed in the preceding table during the FusionAccess maintenance. These operations may result in serious impact on the system.

Forbidden operations-Process Service

- Do not change the default service or startup options in the msconfig system configuration.
- Do not disable HDP services or uninstall related software.
- Do not disable the following processes (Local service、Network service、System)in **Task Manager**.

Forbidden operations-Network

- Do not disable VM NICs. Do not disable or modify network configurations.
- Do not run scripts or commands for modifying route configuration, such as route DELETE.
- Do not delete the following ports from the Windows firewall exception options: 28511, 285512, 28521, and 28522.
- Do not start software or tools that can disable network traffic, such as IPsec.

Other Forbidden Operations

- Do not delete files or folders in the C:\Program Files\Huawei directory.
- Do not enable hibernation on VMs. Hibernation is disabled by default.
- Do not modify the configuration file of the HDP client (access agent).
- Do not run optimization software to clean or optimize registry.

Critical operations (1)

Operation	Risk	Risk Level	Workaround	Follow-Up Operation
Replace an infrastructure server.	Improper operations may cause service interruption.	★★★	Back up data and then replace the server.	Check whether there are uncleared alarms.
Create and associate VMs in batches on the IT adapter (ITA).	If a large number of batch operations are performed during the day, the ITA performance deteriorates and other services may become unavailable.	★★★	1. Create and associate VMs in batches during low-traffic hours. 2. Ensure that resources are sufficient before creating and associating VMs in batches.	Check whether VMs are accessible.
On **System** > **System Configuration** of FusionAccess, perform operations, such as configuring the virtualization environment and desktop components.	Improper operations may cause service interruption.	★★	Record the original configuration information. If a fault occurs, restore the original configuration.	Check whether VMs can be created successfully.
Manually delete VMs.	If a VM is deleted by mistake, data will be lost and services will be interrupted.	★★	Confirm the VM information before deleting a VM.	-

Critical operations (2)

Operation	Risk	Risk Level	Workaround	Follow-Up Operation
Recompose System Disk	Improper operations may result in the loss of user data in the system disk of a linked clone VM.	★★★	Recompose System Disk only when data loss is allowed.	-
Restore System Disk	Improper operations may result in the loss of user data in the system disk of a linked clone VM.	★★★	Restore System Disk only when data loss is allowed.	-
Create scheduled tasks and select policies.	Improper operations may cause service interruption.	★★	Select policies based on service requirements.	Check whether scheduled tasks can be successfully performed.
Configure template types.	Service provisioning fails if the configured template type is not consistent with the required template type.	★★	Confirm the required template type and configure the template type correctly.	Check whether services can be provisioned properly.

Critical operations (3)

Operation	Risk	Risk Level	Workaround	Follow-Up Operation
Adjust or change the clock source.	If the clock source is adjusted or changed, the time on VMs will change, which may cause service interruption.	★★	Adjust or change the clock source during low-traffic hours.	Observe the time difference after the clock source is adjusted or changed.
Update systems concurrently.	A large number of concurrent update operations exhaust CPU resources of servers and congest the storage and network, resulting in slow running of VMs, node restart, or storage faults.	★★★	Update user VMs in different batches.	Check whether there are uncleared alarms.
Concurrently start VMs at work.	If VMs are concurrently started at work, I/O storms are generated, and VMs run slowly.	★★	1. Do not shut down VMs. 2. Get VMs ready using scheduled tasks before employees come to the office.	Check whether there are uncleared alarms.
Play videos concurrently on office VMs.	Playing videos concurrently on office VMs exhausts CPU resources of servers and congests the network, resulting in slow running of VMs, disconnection from VMs, or VM connection failures.	★★	1. Improve the specifications of VMs. 2. Reduce the VM density on a server.	Check whether there are uncleared alarms.

Critical operations (4)

Operation	Risk	Risk Level	Workaround	Follow-Up Operation
Do not restart VMs for a long time.	Memory garbage exists after the OS runs for a long time, resulting in slow running of VMs.	★	Restart VMs every seven days at most.	-
Frequently switch over the active and standby GaussDBs.	The active and standby GaussDB databases may be damaged, and the data may be inconsistent or lost.	★★★	1. Reduce the active/standby GaussDB switchover frequency. 2. During the switchover, do not perform operations such as creating or deleting VMs.	Check whether there are uncleared alarms.
DB exception alarms (1000029 Alarm About Two Active GaussDB Databases, 1001005 HDC Database Exception, and 1004001 Database Server Exception) exist during the GaussDB switchover.	The data in the active and standby GaussDB may be inconsistent and data may be lost.	★★★	1. DB exception alarms cannot exist during the GaussDB switchover. 2. During the switchover, do not perform operations such as creating or deleting VMs.	Check whether there are uncleared alarms.

O&M Tool

O&M Tool	Description	Obtaining Path
Huawei vDesk	Available only for Windows VMs. It is a self-service tool used for system acceleration and display optimization and provides the following tool capabilities: connection inspection, log collection, peripheral assistant, peripheral assistant 2.0, and process information collection.	You do not need to obtain this tool. This tool is installed by default on virtual desktops provisioned using a template. This tool is automatically installed in the virtual desktop template created using the template tool.
Log collection tool	Available only for Linux workspaces. It is a self-service tool for end users to collect logs.	
Maintenance tool	Available only for Linux workspaces. It is a self-service tool for end users to automatically check the workspace status and locate and rectify faults.	

- FusionAccess provides end users and O&M engineers with an O&M tool. The tool can help users rapidly configure and use desktop clients and help O&M engineers easily conduct routine maintenance, significantly improving self-service capabilities and O&M efficiency.

Periodically Restarting Infrastructure VMs

- It is recommended that the infrastructure VMs be restarted every three months. That is, the continuous running duration cannot exceed 120 days.
- Restart infrastructure VMs in idle hours to minimize service interruption.
- During the restart of the active ITA node, service provisioning will be interrupted. Therefore, it is recommended that the active ITA node be restarted when no service provisioning is performed.
- When ITA is deployed with vAG/vLB, vAG/vLB is also restarted when ITA is restarted.
  - If HDP does not pass through the gateway, restarting the active ITA VM does not affect users who have been accessed. New users, however, can be accessed only after the active ITA VM is recovered. Restarting the standby ITA VM does not affect access services.
  - If HDP passes through the gateway, restarting the active or standby ITA VM interrupts user connections and users have to log in again after restart.
- The infrastructure VM restart time cannot be the same as the time of other automatic scheduled tasks. For example, if FusionAccess component backup files are automatically uploaded to the Backup Server at 01:00 every day, the infrastructure VMs cannot be restarted at the same when the backup task is being performed.

- Periodically restart infrastructure VM based on service requirements to ensure the long-term stable running of the system.
- After an infrastructure VM is restarted, wait until the service on the infrastructure VM is started properly before you start the next infrastructure VM.
- Restart Linux infrastructure VMs by running the **reboot** command.

Account Management-Change the password periodically

- FusionAccess account
- Linux OS account
- Accounts for accessing the database
- FTP account
- ITA/WI NBI account
- LiteAS NBI account
- Default LiteAS account
- grub2 account
- Cache account

- Change the default passwords of all users.
- For details about the default FusionAccess account information, see **FusionAccess Account List** in the product documentation of the corresponding version.

Account Management-Changing the Account Lockout Threshold

- To ensure security by avoiding unlimited login attempts, set the login failure thresholds for server accounts of the FusionAccess components.
- If the threshold is set to a large value, the system security is affected. You must set a proper threshold based on actual conditions.

On the FusionAccess web client, choose **System** > **System Configuration** > **Authentication Configuration**. → **The Local Password Authentication** page is displayed. → Change the value of **Account Lockout Threshold (Attempt)**. → Confirm that the modification is successful.

Backup and Restoration-Backup Policy

- System maintenance engineers or technical support engineers manually back up data before performing an important operation on the system, such as system upgrade or critical data modification. If the operation fails, the backup data can be used to restore the system, minimizing the impact on services.
- FusionAccess automatically backs up data (manual backup is not supported) so that services can be restored when a fault occurs.

- The system provides two backup modes, local backup and remote backup. In local backup mode, a backup operation is performed at 03:00 a.m. every day and the storage directory is **/var/vdesktop/backup/**. In remote backup mode, a backup operation is performed at 01:00 a.m. every day and the backup files are uploaded to the storage directory **/var/ftpsite/***ITA name/folder of a component* on the backup server (Backup Server or third-party FTP backup server).
- The backup server (including Backup Server and the third-party FTP backup server) reserves backup data in 10 days. However, when there is insufficient backup space, the system automatically deletes the earliest backup file. The third party controls the retention period and deletion policies for backup data on a third-party FTP backup server.

Backup and Restoration-Restoration Policy

- To restore data of a faulty component, you need to check the time when the fault alarm is generated, and use the latest backup file of the component before the fault on the backup server to restore data.
- Recovery policies vary according to fault scenarios:
  - Recovery by software reinstallation: If the fault is caused by some or all of the software programs on an infrastructure server, you need to reinstall the software and use the backup data on the backup server to restore data.
  - Recovery by OS reinstallation: An OS fault occurs on an infrastructure server. You need to create a server, reinstall the software, and use the backup data on the backup server to restore data.

Quiz

1. How often should a desktop be restarted?
   A. Daily
   B. Weekly
   C. Monthly
   D. No need to restart
2. The FusionAccess backup server stores the backup data generated during the last 10 days.
   A. True
   B. False

- Answers:
  - B
  - A

Summary

- This chapter describes policy management, policy planning, and creation methods of virtual desktops in the FusionAccess desktop cloud. Master the operations related to virtual desktop service adjustment, such as adding desktop users and setting VIP desktops. In addition, you have learned about the O&M process and operations related to FusionAccess.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

Cloud Computing Trends

Foreword

- You have been previously introduced to how virtualization technologies integrate data center resources for better utilization. However, virtualized data centers also face challenges in unified scheduling and management of infrastructures, networks, and storage resources. What are the solutions to these challenges? What is the direction cloud computing is going?
- In this course, you will learn the basic concepts and components of OpenStack and understand edge computing, blockchain, cloud native and artificial intelligence concepts.

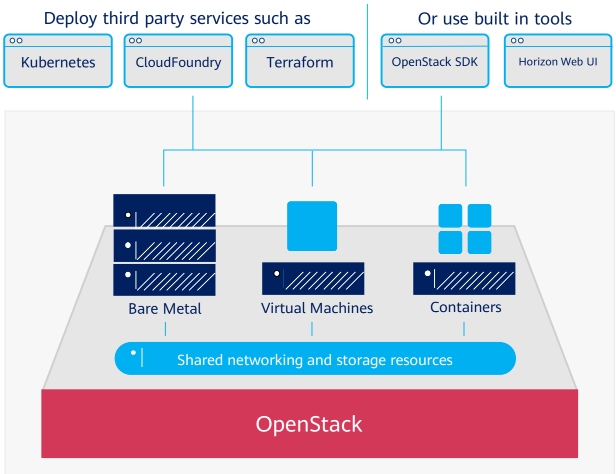
Objectives

- On completion of this course, you will be able to:
  - Understand basic concepts and component architecture of OpenStack.
  - Understand edge computing, intelligent edge, and HUAWEI CLOUD IEF.
  - Understand blockchain and HUAWEI CLOUD BCS.
  - Understand cloud-native, cloud-native applications, and HUAWEI CLOUD UCS.
  - Understand artificial intelligence and HUAWEI CLOUD ModelArts.

Contents

1. **OpenStack Overview**
2. Overview of Emerging Technologies

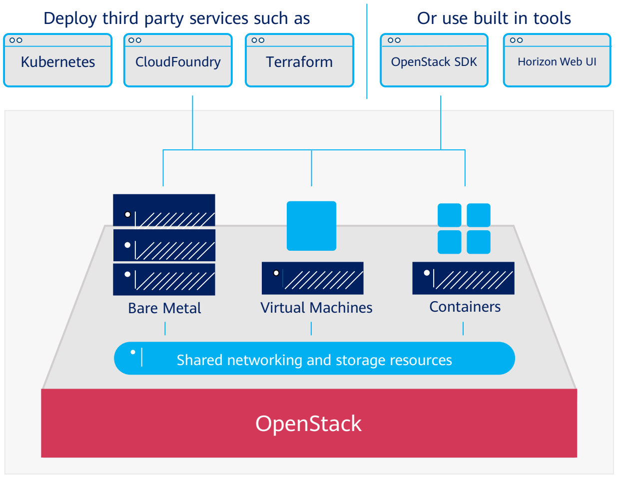
What Is OpenStack?



- It provides a cloud infrastructure for virtual machines (VMs), bare metal, and containers.
- It controls large pools of compute, storage, and network resources.
- It manages all resources through APIs or a dashboard.

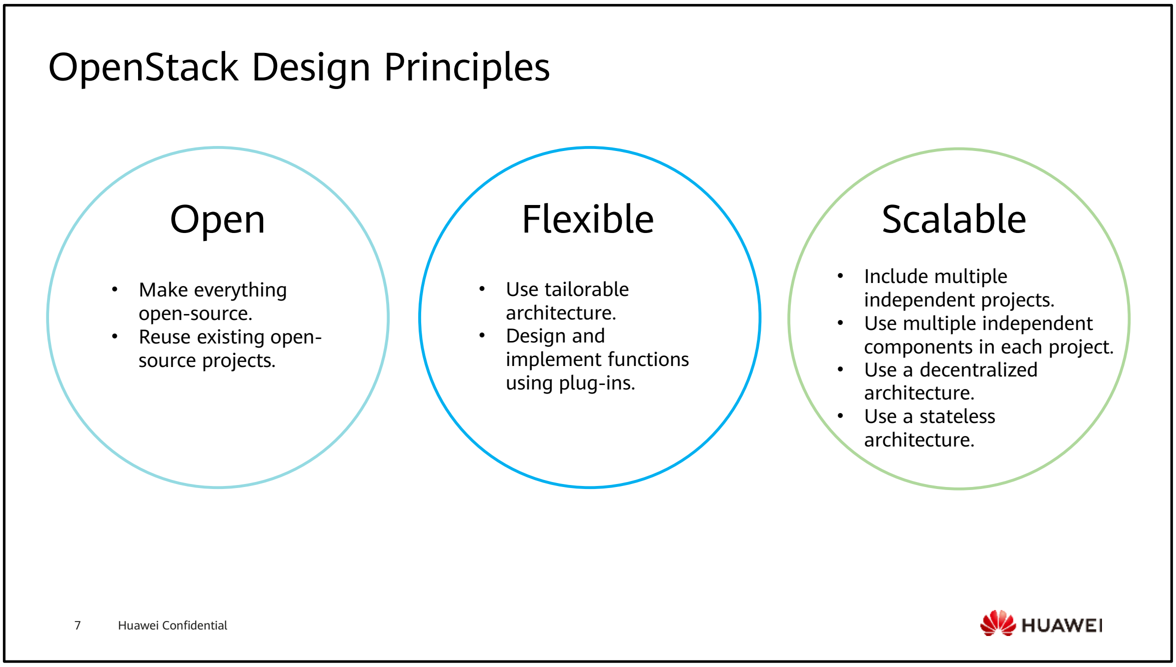
- OpenStack is a cloud operating system that controls large pools of compute, storage, and network resources throughout a data center, all managed and provisioned through APIs with common authentication mechanisms. A dashboard is also available, giving administrators control while empowering their users to provision resources through a web interface.

What Can OpenStack Do?



- OpenStack provides an Infrastructure as a Service (IaaS) solution through a variety of complementary services. Each service offers an Application Programming Interface (API) to facilitate integration.
- The OpenStack project is an open source cloud computing platform that supports all types of cloud environments. The project aims for simple implementation, massive scalability, and a robust feature set.

- OpenStack is a community, a project, and open-source software application. It provides open-source software for building public and private clouds. It also provides a cloud platform or tool set to deploy clouds and helps organizations run clouds that provide services for virtual computing or storage, providing scalable and flexible cloud computing for public clouds, private clouds, big clouds, and small clouds.
- As an open-source cloud computing management platform, OpenStack consists of multiple main components. OpenStack supports almost all types of cloud environments. It aims to provide a cloud computing management platform featuring simple implementation, massive scalability, a rich set of functions, and unified standards. OpenStack provides an Infrastructure as a Service (IaaS) solution through a variety of complementary services. Each service provides an API for integration.



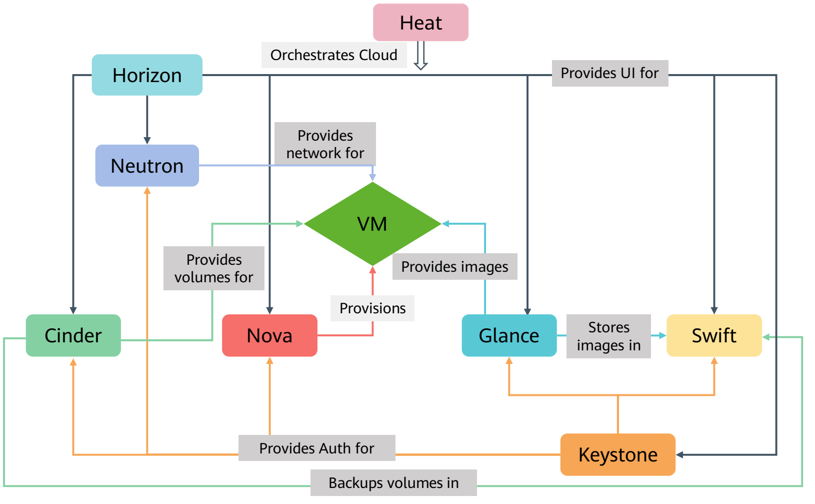
- Open:
    - The source code and the design and development processes are open.
    - Do not reinvent the wheel but stand on the shoulders of giants.
    - No irreplaceable private or commercial component is used.
- Flexible:
    - Tailored architecture and customizable component scope.
    - A large number of drivers and plug-ins.
    - Easy configuration of system functions and features based on configuration items.
- Scalable:
    - Loosely coupled architecture: Components communicate with each other through RESTful APIs, and message bus communication is used within a component.
    - Decentralized architecture: Core components do not have central nodes, effectively preventing single points of failure.
    - Stateless architecture: Components do not have local persistent data. All persistent data is stored in the database.

OpenStack vs. FusionCompute

Feature	OpenStack	FusionCompute
Definition	Fully open-source cloud computing platform	Business cloud computing platform
Open source	Maintained and developed by global developers, users can use all functions.	Some features require a license fee to use
Architecture	Consists of multiple components, each of which can be configured and managed separately	All-in-one cloud computing platform, all functions are packaged together, and each component cannot be configured or managed separately.
Virtual resource pool management	Virtualized resource pool management for computing, storage, and network resources	VRMs (two active/standby) are used for computing, storage, and network management of virtual resource pools.
Multi-tenancy and cloud service automation	The cloud service management layer implements multi-tenant, metering, and approval management, and provides various IaaS-layer cloud service automation.	Multi-tenancy and cloud service automation are not supported.
CMP layer (ManageOne)	The CMP layer (ManageOne) is not supported.	Supports the CMP layer (ManageOne) to implement multi-tenant, VDC, metering, and approval management, and provides various IaaS-layer cloud service automation.

HUAWEI

Service Interactions for Creating a VM in OpenStack

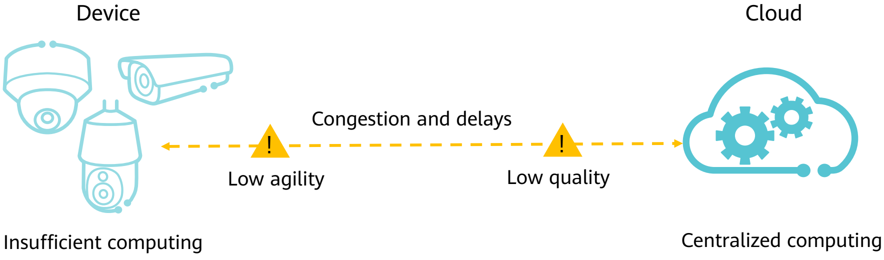


- Horizon provides a web-based self-service portal to interact with OpenStack underlying services, such as starting an instance, assigning IP addresses, and configuring access control.
- Nova manages the lifecycles of computing instances in the OpenStack environment. On-demand response includes VM creation, scheduling, and reclamation.
- Neutron provides network services for other OpenStack services and provides APIs for users to define and use networks. The plug-in architecture is compatible with many network providers and technologies.
- Swift stores and retrieves unstructured data through HTTP-based RESTful APIs. It runs on a scalable architecture and supports data replication and fault tolerance.
- Cinder provides persistent block storage for running instances.
- Keystone provides authentication and authorization services for other OpenStack services and provides an endpoint directory for all OpenStack services.
- Glance stores and retrieves VM disk images. OpenStack computing uses this service to deploy instances.
- Ceilometer provides monitoring and measurement for OpenStack charging, baseline, scalability, and statistics.
- Heat orchestrates multiple cloud applications through OpenStack REST APIs and CloudFormation-compatible queue APIs and provides local templates or AWS CloudFormation templates.

Contents

Background of Edge Computing

- The Internet of Everything (IoE) era is coming rapidly. The popularization of 5G networks leads to rapid growth of network edge devices and data volume.
- The computing capability of network edge devices is insufficient. When the devices are aggregated in a centralized data center, real-time response, network stability, and data security are challenged.

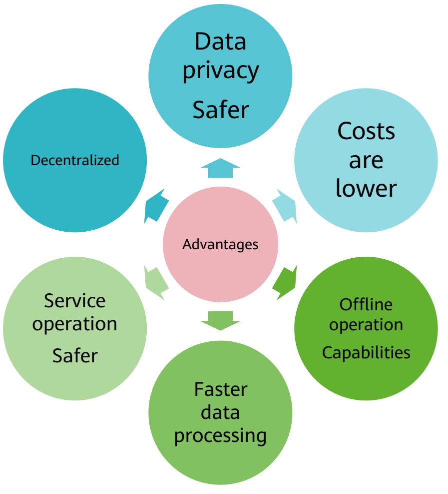


- When computing is performed at the edge, the complexity of monitoring and scheduling edge resources increases exponentially with the expansion of the scale, which directly affects the overall computing efficiency. Therefore, it is urgent to improve the cloud-edge collaboration computing and management capabilities of edge devices and applications.

What is Edge Computing?

- Edge computing is a distributed computing architecture, which moves the computing of applications, data, and services from the network center node to the network logical edge node for processing. Edge computing breaks down large services that are originally processed by the central node into smaller and easier-to-manage parts and distributes them to edge nodes for processing. The edge node is closer to the user terminal device, which can accelerate the data processing and transmission speed and reduce the delay. Edge computing provides intelligent analysis and processing services close to data sources, reducing latency, improving efficiency, and improving security and privacy protection.

Advantages of Edge Computing

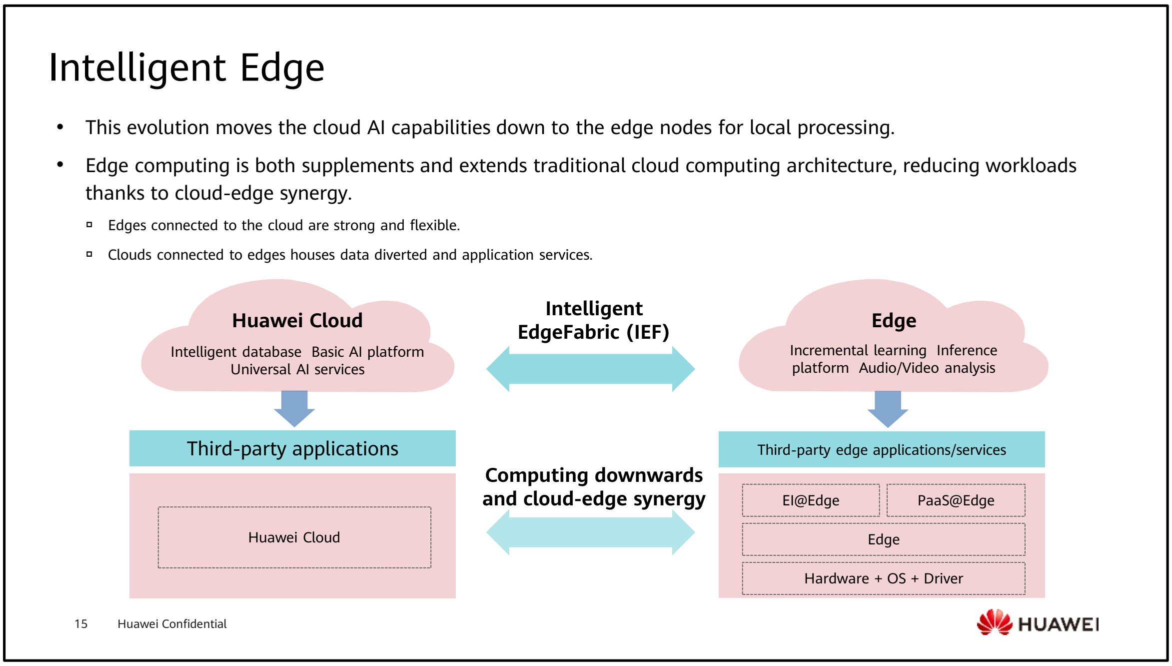


- Data privacy safer: with edge computing, data can be kept where it is produced, used, and owned.
- Costs are lower: reduced data transfer and central storage significantly reduces network and cloud costs.
- Faster data processing: direct processing on edge devices, rather than sending data to the cloud and processing.
- Offline operation capability: with edge computing, devices run independently from network/cloud connections.
- Decentralization: edge devices can communicate directly with each other. This decentralized edge calculation method is more efficient because of the short distance and the ability to combine power and information from multiple devices, increasing elasticity.
- Service operation safer: as the number of connected devices increases, the possibility of being attacked increases. Traditional cloud computing is centralized and is more vulnerable to DDoS attacks and power outages. However, edge computing is distributed across devices and data centers for processing and storage, which makes it difficult for a single interruption to destroy a network.

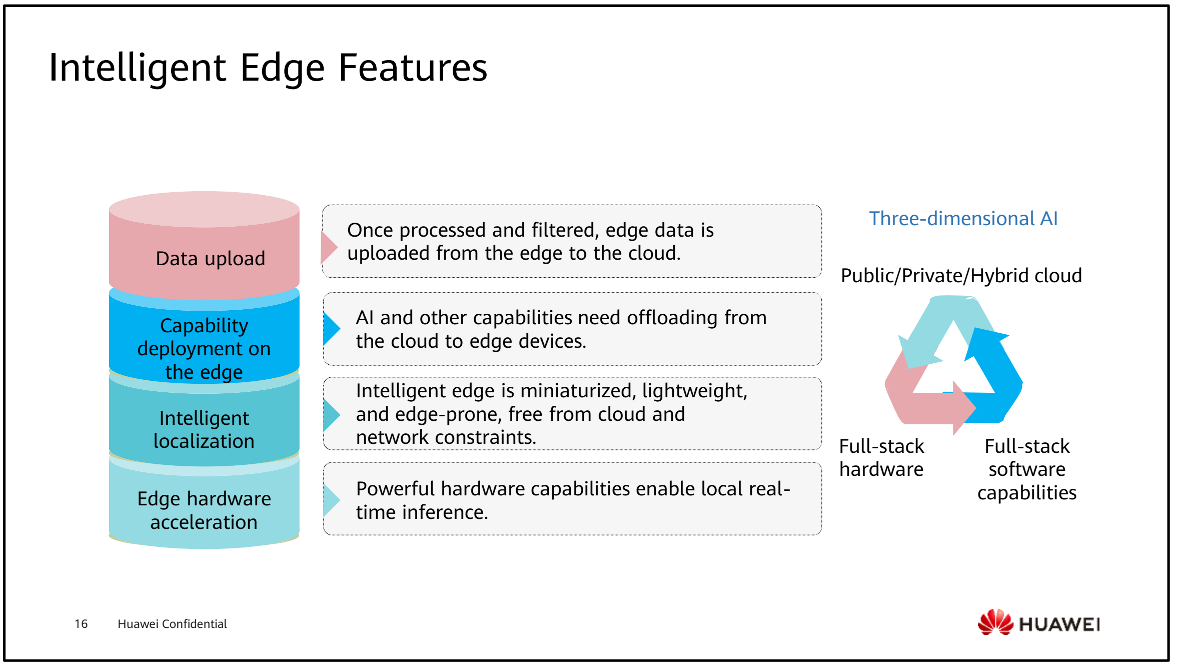
Edge Computing and Cloud Computing

- Disadvantages of cloud computing:
  - Big Data Transmission Problems
  - Timeliness of data processing
  - Privacy and energy consumption issues
- Advantages of edge computing:
  - More nodes load traffic, enabling faster data transmission
  - Closer to terminal devices, more secure transmission, and more instant data processing
  - More distributed nodes have less impact than cloud computing failures and address device cooling issues
- Edge computing is a supplement and extension of cloud computing.

- Cloud computing is the interaction between people and computing devices, while edge computing is the interaction between devices and indirectly serves people. Edge computing can process a large amount of instant data, and cloud computing can finally access the history or processing results of the instant data and summarize and analyze it. Therefore, edge computing is a supplement and extension of cloud computing.



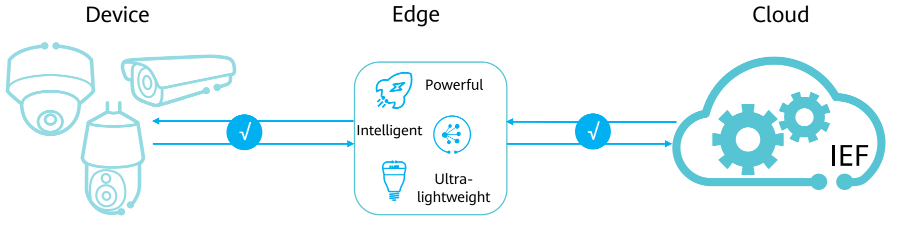
- Cloud computing capabilities are centralized and it takes a long time to deliver computing results from the cloud to devices such as cameras and sensors. As a result, performing computing only in the cloud will cause high network latency, network congestion, and service quality deterioration when real-time computing is required. However, the computing power of local devices is far lower than that in the cloud. This is where edge computing comes in. By deploying edge nodes near devices, computing capabilities are extended to the edge to meet real-time data processing needs.
- Intelligent EdgeFabric (IEF) manages edge nodes, extends cloud applications to edge nodes, and associates edge and cloud data to enable remote control, data processing, and intelligent analysis and decision-making of edge computing resources. IEF also provides an integrated edge computing solution that features edge-cloud synergy, which allows for unified on-cloud O&M such as device/application monitoring and log collection.



- The intelligent edge needs more than a single technology.
- The framework and software stack of intelligent edge computing show features of different layers: the underlying hardware acceleration; the intelligent localized and lightweight technologies at the middle layer; edge-cloud synergy at the upper layer, such as capability deployment on edges, anonymized data upload, and device management.
- Full-stack hardware and software and public/private/hybrid cloud computing are essential capabilities.

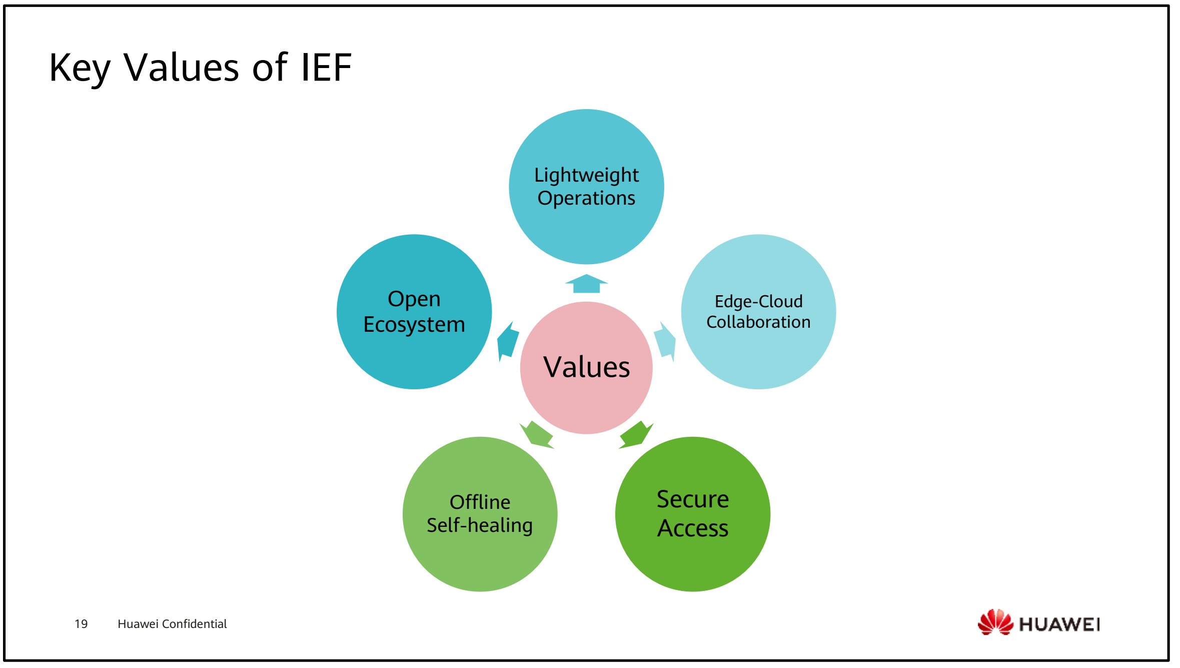
HUAWEI CLOUD IEF

- Based on the KubeEdge and Kubernetes ecosystem, HUAWEI CLOUD Intelligent EdgeFabric applies cloud-native technologies to edge computing, providing enterprises with a cloud-native edge computing platform with ultra-lightweight, edge intelligence, and powerful computing power.



- Kubernetes (also known as "k8s" or "kube") is a mainstream open-source container orchestration platform. You can use it to deploy and manage containerized application software systems on a large scale, facilitating container scheduling and orchestration. Kubernetes has a large and fast-growing ecosystem with widely available services, support, and tools.
- KubeEdge: a cloud-native edge computing platform, or Kube+Edge. As the name suggests, Kube+Edge relies on Kubernetes' container orchestration and scheduling capabilities to implement edge-cloud synergy, computing sinking, and smooth access of massive devices.
- Cloud Native is a software architecture and development methodology designed to build, deploy, and run scalable distributed applications. It's a way to build and run applications in the cloud, making them more efficient, scalable, and flexible. Cloud native concepts include containerized encapsulation, microservice architecture, automated deployment, continuous integration, and continuous delivery.
- Cloud computing is centralized and is far away from terminal devices (such as cameras and sensors). For computing requirements that require high real-time performance, deploying computing on the cloud will cause problems such as longer network delay, network congestion, and service quality deterioration. Terminal devices, however, usually have insufficient computing capabilities and cannot be compared with the cloud. In this case, edge computing is generated according to the requirements. By establishing an edge node close to the terminal device, a cloud computing capability is extended to an edge node close to the terminal device, thereby solving the foregoing problem.

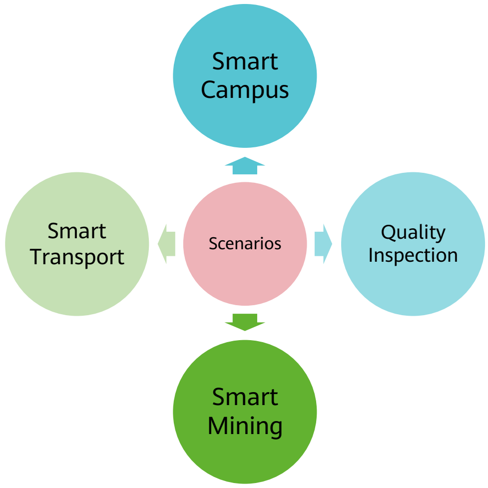
- IEF manages customers' edge nodes, extends cloud applications to the edge, and associates edge and cloud data to meet customers' requirements for remote management, data processing, analysis, and decision-making of edge computing resources. Provides unified O&M capabilities such as edge node/application monitoring and log collection on the cloud, providing enterprises with an integrated edge computing solution featuring edge-cloud synergy.



- Lightweight Operations
    - Container and function management available for just 128MB of edge hardware.
    - Lean O&M, quick access to millions of nodes, unified monitoring and O&M.
- Edge-Cloud Collaboration
    - Cloud-based training and edge inference without high bandwidth consumption and 40+ AI algorithms extended to the edge;
    - Interconnection with 10+ Huawei cloud services.
    - Applications are intelligently scheduled to edge clusters using set policies.
- Secure Access
    - Flexible edge-cloud network access, including VPN, Direct Connect, and Internet access.
    - Cloud-edge-device communication secured by multi-level certificates(one certificate for one device).
- Offline Self-healing
    - Services are managed locally in case of disconnected or unstable edge network.

- Open Ecosystem
  - Intelligent Edge Marketplace(IEM) shares industry environment with edge application developers, hardware providers, and solution integrators to form an edge AI ecosystem.
  - Heterogeneous hardware such as Kunpeng, Ascend, x86, and GPU.

IEF Application Scenarios



- Smart Campus: video surveillance and AI analysis ensure security with technology instead of labor for better management efficiency and user experience.
- Quality Inspection: industrial vision is integrated with AI to make inspections more accurate, efficient, and cost-effective.
- Smart Mining: the Mine Brain solution is built on edge computing, AI, IoT devices, and big data analysis to summarize and monitor coal production, transportation, and warehousing statuses in real time.
- Smart Transport: Edge-intelligent vehicles sense their environment, preventing congestion and accidents for better safety and efficiency.

Contents

Background of Blockchain Generation

- It dates back to 2008, when a man named Satoshi Nakamoto proposed the concept of Bitcoin in a paper. Bitcoin is a blockchain-based cryptocurrency that breaks the boundaries of traditional financial systems and provides a decentralized digital currency transaction. As the underlying technology behind Bitcoin, blockchain solves the trust and security problems in traditional financial systems through the operation of distributed accounting and encryption algorithms. Blockchain has attracted wide attention due to its transparency and tamper-proofness and has begun to be used in other fields, such as supply chain management, Internet of Things, medical records, etc.

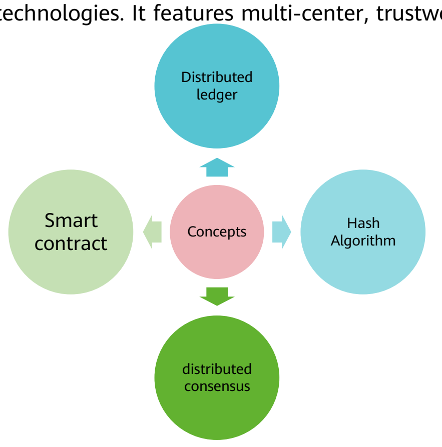
- The background of blockchain can be said to address the limitations of existing financial and data management systems and to provide a new solution for building a decentralized, transparent and secure trading environment.

What Is Blockchain?

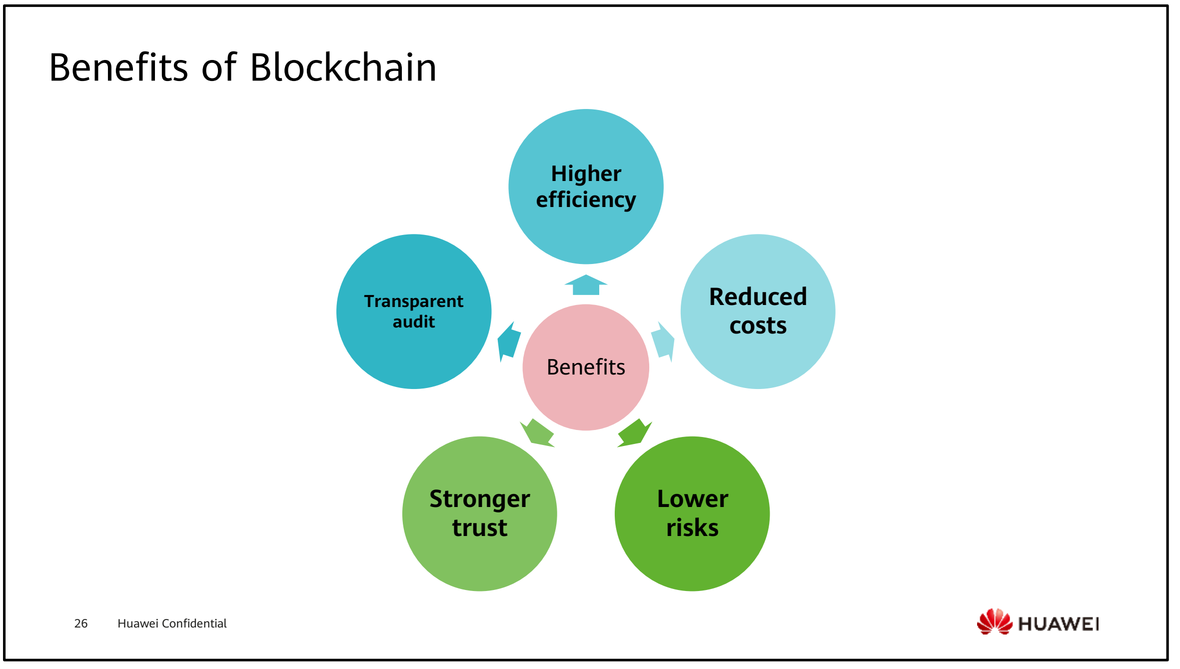
- Narrow sense: A blockchain is a chained data structure that combines data blocks in chronological order and is cryptographically guaranteed to be tamper-proof and unforgeable distributed ledgers.
- Broadly speaking, blockchain technology is a new distributed infrastructure and computing paradigm that uses blockchain data structures to verify and store data, uses distributed node consensus algorithm to generate and update data, uses cryptography to ensure data transmission and access security, and uses smart contract composed of automated script codes to program and operate data.

Blockchain Technology Concepts

- The blockchain technology is a combination of distributed ledgers, consensus algorithm, security and privacy, and smart contract technologies. It features multi-center, trustworthy consensus, tamper-proof, and traceability.



- Distributed ledger: A database that is shared, replicated, and synchronized among network members. It records transactions (such as asset or data exchange) between these members without spending time and money for ledger reconciliation.
- Cryptography (or hash algorithm): The hash value of a digital content segment can be used to verify its integrity. Any modification to digital content significantly changes its hash value. A qualified hash algorithm easily obtains this value from digital content while preventing back-calculation of the original digital content from the value.
- Distributed consensus: A system's independent participants must achieve majority consensus on a transaction or operation. Examples include verifying double-spending transactions, validating transactions, and determining whether to write verified data to the existing ledger.
- Smart contract (or chaincode): This runs on a blockchain and is automatically triggered by specific conditions. It is an important way to implement service logic when using a blockchain. Due to the nature of blockchains, the execution results of contracts cannot be forged or tampered with, and their reliability is assured.

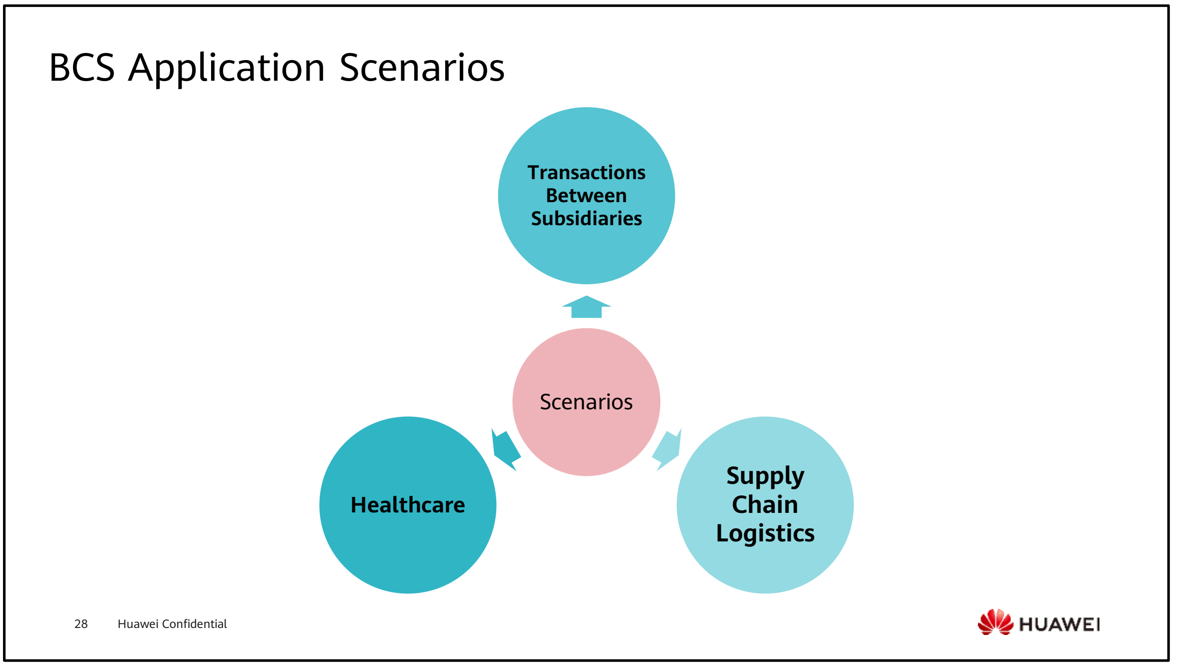


- **Higher efficiency**: Builds a trusted multi-party collaboration platform to reduce disputes and improve transaction efficiency.
- **Reduced costs**: Reduces extra costs and the participation of third parties.
- **Lower risks**: Precludes the possibility of tampering to reduce risks of frauds and network errors.
- **Stronger trust**: Builds up trust between transaction participants using shared ledgers, processes, and records.
- **Transparent audit**: Audit institutions can audit the immutable ledgers at any time.

HUAWEI CLOUD BCS

- HUAWEI CLOUD Blockchain Service (BCS) is a high-performance, high-availability, and high-security blockchain platform service for enterprises and developers. It helps enterprises and developers quickly create, deploy, and manage blockchain applications on HUAWEI CLOUD at a low cost. Lowers the threshold for users to use blockchain, enables users to focus on their own service development and innovation, and implements fast service chaining.
- HUAWEI CLOUD BCS supports the creation of Hyperledger Fabric Enhanced Edition and HUAWEI CLOUD BCS instances, including user management, node management, and O&M monitoring modules, helping users quickly create, manage, and efficiently maintain blockchain networks and providing enterprise-level blockchain systems for upper-layer applications.

- For enterprises, it is not easy to develop blockchain-based services. They need to master the complex underlying technologies of blockchain, and the threshold for using blockchain is high. Building a blockchain system is complex, complicated, time-consuming, and costly. Unable to focus on the development and innovation of upper-layer service applications.
- Hyperledger Fabric Enhanced Edition: With Hyperledger Fabric as the kernel, HUAWEI CLOUD full-stack trusted capabilities, including ECSs, enterprise-level containers, security, and artificial intelligence services, enhances reliability, performance, and privacy protection while maintaining seamless community interconnection. Meets enterprise- and financial-class business requirements.
- HUAWEI CLOUD blockchain engine: Based on BCS's self-developed blockchain kernel and trusted hardware, HUAWEI CLOUD blockchain engine features high security, high performance, high scalability, and strong privacy protection, meeting enterprise- and financial-level trustworthiness and collaboration requirements.



- **Transactions Between Subsidiaries:** BCS provides end-to-end (E2E) audit support for inter-subsidiary transactions by building a collaboration consortium with subsidiaries of a multinational company and audit organizations involved, developing trust and eliminating reconciliation and discrepancies between the transaction parties.
- **Supply Chain Logistics:** Manufacturers, warehousing institutes, logistics providers, and customers can use BCS to comprise collaboration consortia and use IoT technologies to record all the logistics information of goods, including production, warehousing, line haul transportation, reselling, and local logistics. The consortia break down information silos, improve circulation of information, and build trust between parties.
- **Healthcare:** BCS helps healthcare institutions, third-party organizations, and supervision departments to form a collaboration consortium. Healthcare information silos are broken down using electronic medical records that cannot be tampered with to protect privacy. This builds trust between doctors and patients and provides comprehensive health and medical care information for telemedicine and referral.
- In addition to the preceding application scenarios, BCS also applies to the following scenarios/industries: smart city, IoT device management, food safety, data application, identity authentication, financial insurance, and information proof.

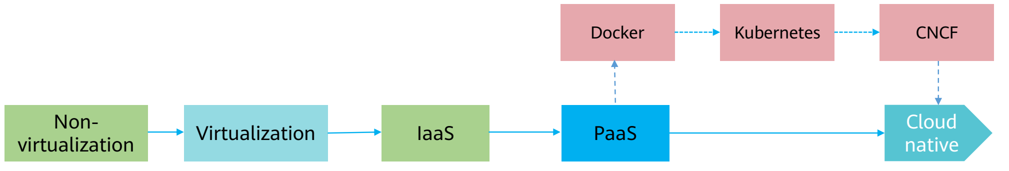
Contents

Background of Cloud Native Generation

- Similar to the above emerging technologies, any new technology/methodology is driven by practical requirements. Cloud native is proposed to adapt to distributed architectures in today's hot and complex application systems.
- As the service scale expands, the monolithic architecture is changed to the distributed architecture. Large applications are split into multiple small applications by vertical or horizontal segmentation. This is almost an inevitable choice to increase system capacity and enhance system availability.
- The distributed architecture facilitates user development and implementation, narrows the impact scope of faults, and greatly enhances the scalability of the development system. However, distributed distribution brings these advantages and many problems. For example, the release frequency increases, the deployment becomes more complex, the system architecture design becomes more difficult, and the response time becomes an important factor due to the introduction of network communication. In addition, the O&M difficulty increases exponentially.

Cloud Computing and Cloud Native

- Cloud native is the surest path to cloud migration.
- Cloud native makes the most of cloud.
- Applications, platforms, and systems can all be cloud native.



- Pivotal explicitly introduced the concept of cloud native in 2015, stating that cloud native is a way to build and run applications that take advantage of the benefits of cloud computing.
- Cloud computing is the mainstream IT platform and lays a foundation for cloud native development. Cloud native is the development trend of cloud computing services and the upgrade of cloud computing.

Definition of Cloud Native

- Cloud native technologies empower organizations to build and run scalable applications in public, private, and hybrid clouds. Features such as **containers, service meshes, microservices, immutable infrastructure, and declarative APIs** best illustrate this approach.

  — CNCF

- As can be seen from the positioning of cloud native, cloud native contains a large number of new PaaS layer technologies and new development concepts, which are the shortest path to unlock the value of cloud computing and promote the further upgrade of cloud computing. CNCF is also working to standardize cloud-native technologies, providing users of cloud-native technologies and products with a standard interface to use cloud services while avoiding vendor lock-in. Cloud native is not only a re-upgrade of the application architecture that uses the cloud, but also a re-upgrade of the technologies and cloud services of the cloud platform.

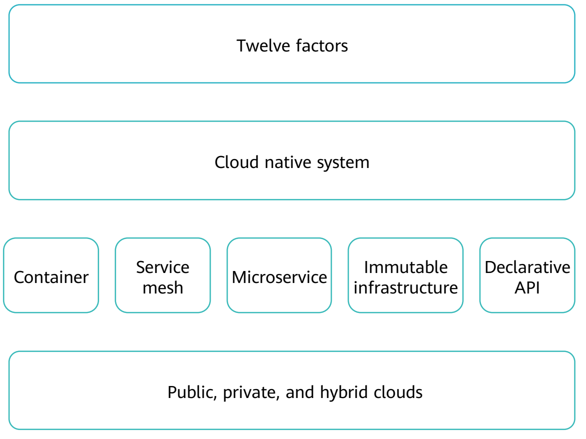
- CNCF: Cloud Native Computing Foundation (CNCF) was established in July 2015 by Google in collaboration with the Linux Foundation and other technology companies (such as IBM, Microsoft, and Red Hat).
- Container: Containerization is a virtualization technology, also called operating system level virtualization (OS level virtualization). This technology virtualizes the OS kernel and allows user space software instances to be divided into several independent units and run in the kernel. Instead of just one single instance running. This software instance is also called a container.
- Microservice: A software architecture style. It combines complex large-scale applications in a modular manner based on small building blocks that focus on a single responsibility and function. The functional blocks communicate with each other using the API set of language-independent (Language-Independent/Language agnostic).
- Service grid: decouples communication between services from service processes and provides services in sidecar mode. In addition, the data plane and control plane are decoupled.
- Immutable infrastructure: Once an instance of any infrastructure is created, it becomes read-only. If the instance needs to be modified or upgraded, it will be replaced with a new instance.
- Declarative APIs are deployed and controlled by describing the final status of the system, compared with imperative APIs.

Features of Cloud Native

Cloud Native	Cloud Native and Platform	Cloud Native Application	Non-Cloud Native System
Auto scaling	Container-based auto scaling	Stateless and lightweight	No auto scaling
Fault tolerance	Container-based, automatic failover	Graceful shutdown	Infrastructure-based fault tolerance
Automation	Cloud native O&M	Dialing test APIs	-
Self-service	Declarative APIs	-	-
Observability	Platform collectors	Non-intrusive	Tracing point, non-intrusive
Immutable infrastructure	Container images	Containerization	Snowflake servers
Agile services	Container, service mesh, and DevOps	Microservice	Monolithic applications on VMs
Easy of use	Declarative APIs and service mesh	-	Imperative APIs
Use of cloud services; logic-focused coding	Cloud native, service mesh, and ecosystem	-	Code or framework
O&M for middleware and stateful applications	Automated O&M with Operators	-	Manual O&M or automated O&M scripts

- Cloud-native applications need to be deployed in the cloud environment, but applications deployed in the cloud environment are not necessarily cloud-native applications.
- Cloud-native applications are scalable, fault-tolerant, and observable.

Cloud Native Architecture



- Twelve elements of cloud-native applications: baseline code, declarative dependency, configuration management, back-end services, build release and running, processes, port binding, concurrency, ease of processing, equivalence between development environment and online environment, logs, and management processes.
- Microservice architecture: Services interact with each other in a highly cohesive and low-coupling manner.
- Container: As the best carrier of microservices, container provides a self-contained packaging mode.
- Container orchestration: solves the problem of microservice deployment in the production environment.
- Service network: As the infrastructure, it solves the communication between services.
- Immutable infrastructure: improves release efficiency and facilitates rapid expansion.
- Declarative APIs: Make the system more robust.

Introduction to Cloud Native Applications

- Cloud native applications are **purpose built for the cloud model**. These applications—built and deployed in a rapid cadence by **small, dedicated feature teams** to a platform that offers easy scale-out and hardware decoupling—offer organizations greater **agility, resilience, and portability** across clouds.

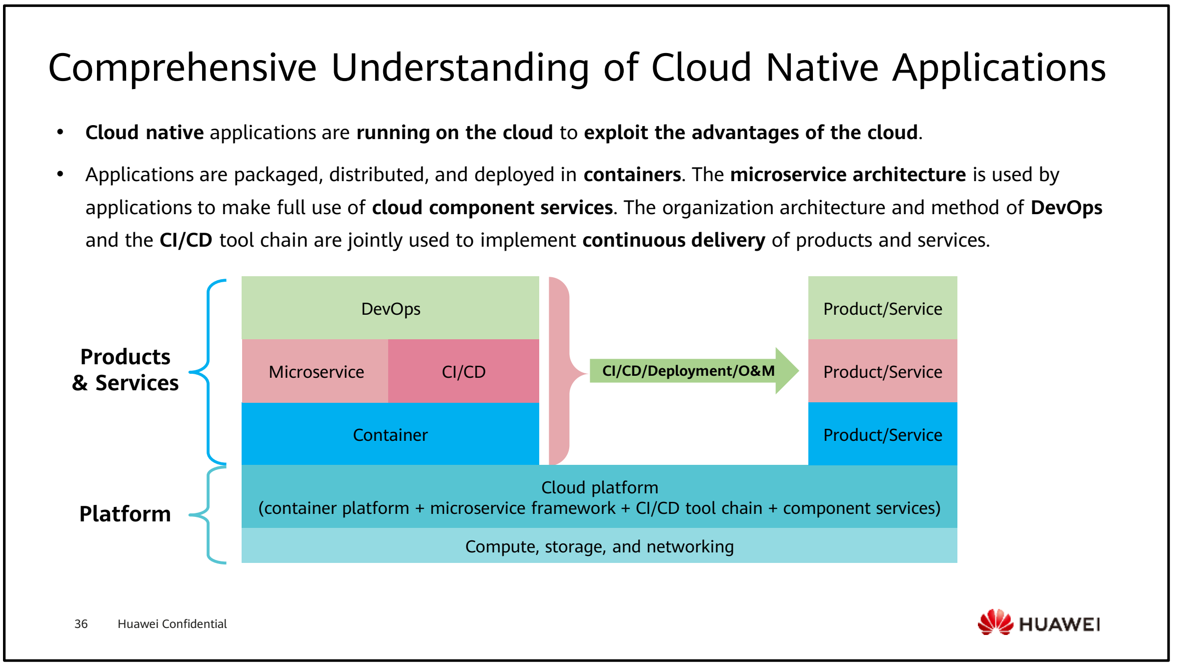
  — Pivotal

  https://pivotal.io/de/cloud-native

- Cloud-native applications are a collection of **small, independent, and loosely coupled services**. They are designed to deliver well-recognized business value, like the ability to rapidly incorporate user feedback for **continuous improvement**. In short, cloud-native app development is a way to speed up how you build new applications, optimize existing ones, and connect them all. Its goal is to **deliver apps users want** at the pace a business needs.

  — Red Hat

  https://www.redhat.com/en/topics/cloud-native-apps



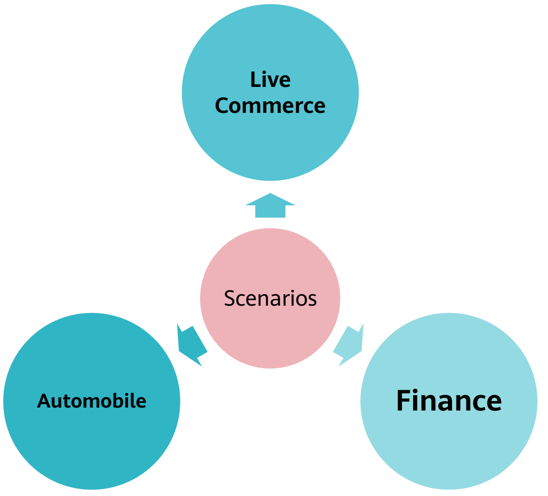
- Cloud native is an approach and practice. Cloud native applications are the practice results of cloud native.
- The platform layer provides cloud native technical support.
- The product and service layer incorporates four key technologies and organization structure of the cloud native architecture for continuous delivery.

HUAWEI CLOUD UCS

- UCS(Ubiquitous Cloud Native Service) is the first distributed cloud native product in the industry. It provides consistent experience in cloud native application deployment, management, and ecosystem. Cloud native applications can freely run across regions and clouds with intelligent traffic distribution.

- Running on Karmada, CNCF's first multi-cloud container orchestration project, UCS enables you to run cloud native applications across clouds or regions, no matter whether they are running on Huawei Cloud (CCE and CCE Turbo clusters), partner clouds (CCE clusters), other clouds (other cloud vendors' Kubernetes clusters), or on-premises infrastructure (clusters provided by Huawei Cloud and clusters deployed by yourself). UCS extends cloud native to central regions, hotspot areas, customer premises, and service sites.

HUAWEI CLOUD UCS Application Scenarios



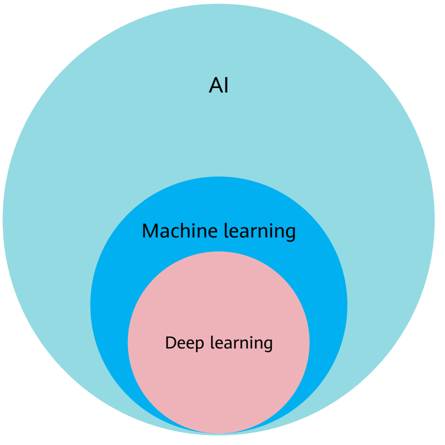
- **Live Commerce:** Nearby access and intelligent scheduling.
- **Finance: Unified** application ecosystem and multi-cloud cluster collaboration.
- **Automobile:** Flexible vehicle networking and on-demand resource supply.

Contents

What Is Artificial Intelligence?

- "Artificial" in artificial intelligence (AI) means that it is designed by and is created for humans.
- AI is a scientific discipline that studies and develops theories, techniques, and application systems used to simulate and extend human intelligence. The term was first coined by John McCarthy in 1956, who defined it as the "science and engineering of making intelligent machines, especially intelligent computer programs". The very premise of AI technology is to enable machines to learn from collected data, and make human-like decisions.
- Today, AI has become an interdisciplinary course that involves various fields.

Relationship Between AI, Machine Learning, and Deep Learning (1)



- Artificial intelligence, machine learning and deep learning are closely related concepts.
- Artificial intelligence is a subject that studies how to enable computers to simulate human intelligence. Machine learning is one of the ways to realize artificial intelligence. It allows machines to automatically learn and extract rules from a large amount of data to predict unknown data.
- Deep learning is an algorithm of machine learning. It uses deep artificial neural networks to learn knowledge, and usually has good performance for complex, large-scale, and high-dimensional data. It can be said that deep learning is one of the most important breakthroughs in the field of machine learning and one of the key technologies to realize artificial intelligence.
- Therefore, it can be said that machine learning is the way to realize artificial intelligence, and deep learning is an efficient algorithm in machine learning.

Relationship Between AI, Machine Learning, and Deep Learning (2)

- AI is a scientific discipline that studies and develops theories, techniques, and application systems used to simulate and extend human intelligence.
- Machine learning (ML) refers to the ability of computers to learn, simulate, or implement human behavior to acquire new knowledge or skills, and continuously update existing knowledge structures to improve performance.
- Deep learning (DL) is a research field in ML and originates from artificial neural network (NN) studies. Multilayer perceptron (MLP) is a deep learning structure. Deep learning uses higher level features derived from the lower level features to form a hierarchical representation, in which it simulates the mechanisms of the human brain to interpret data, such as images, voice, and text.

- The term "artificial intelligence" was previously used to describe machines that imitate and demonstrate "human" cognitive skills related to human thinking.
- Machine learning algorithms build models based on sample data (training data) to make predictions or decisions without explicit rules.
- Deep learning (DL) is a research field in ML and originates from artificial neural network (NN) studies. Multilayer perceptron (MLP) is a deep learning structure. Deep learning uses higher level features derived from the lower level features to form a hierarchical representation. Deep learning aims to establish neural networks that simulate the human brain to analyze and interpret data, such as images, voice, and text.

Types of AI

- Strong AI:
  - This hypothesis aims to create intelligent machines that replicate human functions, such as reasoning and problem-solving, and are perceptive and self-conscious. Strong AI will be able to think independently and teach itself to solve new problems, and have its own values and worldviews, and will even have the same instincts as creatures, such as survival and safety needs. In a sense, strong AI can be seen as a new species.
- Weak AI:
  - Weak AI aims to build intelligent machines that can perform specific tasks but rely heavily on human interference. These machines may seem intelligent but are not self-conscious.

- A key counter of AI is to achieve a superhuman level in challenging fields through self-learning without any prior knowledge.
- Strong AI can compete with humans in all aspects. Therefore, it aims to enable robots to implement human-like capabilities in all aspects rather than a specific field. Strong AI can think, make plans, solve problems, perform abstract thinking, understand complex concepts, quickly learn, and learn from experience. Currently, it is believed that if we can simulate the human brain and copy all its neurons and synapses on the same scale, strong AI will naturally occur.
- Now we are in the weak AI phase. The emergence of weak AI alleviates human intellectual labor, similar to advanced bionics. Both AlphaGo and robots that can write press releases and novels fall in the weak AI phase because they are better than humans only in some ways. The roles of data and computing power are self-evident in the era of weak AI, and they promote the commercialization of AI. In the era of strong AI, these two factors are still critical. At the same time, the research on quantum computing by technology giants like Google and IBM also provides powerful support for humans to enter the era of strong AI.

What Is the Purpose of AI Development

- AI development aims to centrally process and extract information from volumes of data to summarize internal patterns of the study objects.
- Massive volumes of collected data are computed, analyzed, summarized, and organized by using appropriate statistics, machine learning, and deep learning methods to maximize data value.

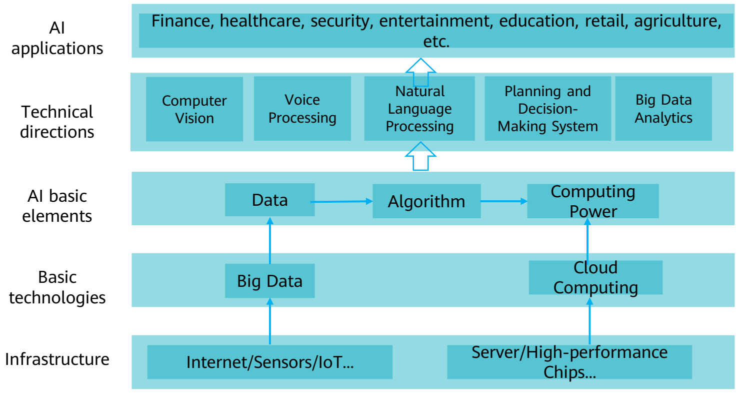
Basic Process of AI Development

Determine the Objective → Prepare Data → Train a Model → Evaluate the Model → Deploy the Model

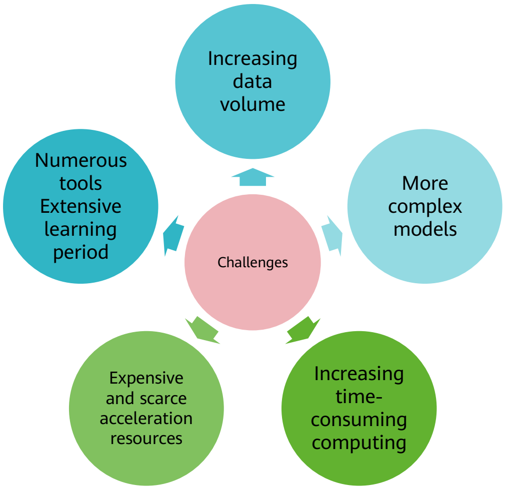
- The basic process of AI development includes the following steps: determining an objective, preparing data, and training, evaluating, and deploying a model.

AI Industry Ecosystem

- Data, algorithms, computing power, and application scenarios are the basic elements of AI applications. We must combine AI with premium cloud computing, big data, and IoT to facilitate our intelligent society.



AI Development Challenges



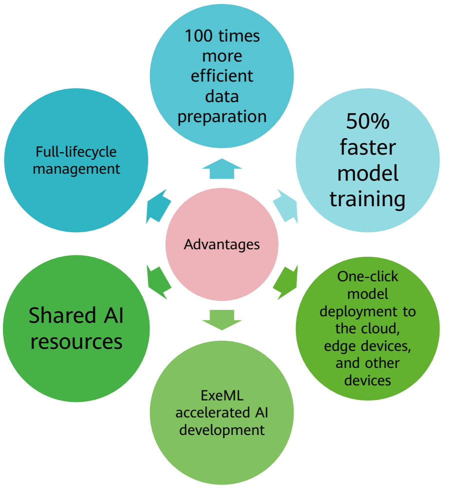
HUAWEI

Huawei AI development platform ModelArts

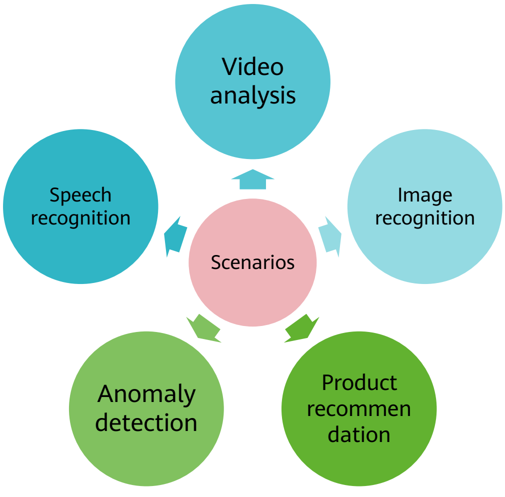
- ModelArts is a one-stop AI development platform geared toward developers and data scientists of all skill levels. It enables you to rapidly build, train, and deploy models anywhere (from the cloud to the edge), and manage full-lifecycle AI workflows. ModelArts accelerates AI development and fosters AI innovation with key capabilities, including data preprocessing and auto labeling, distributed training, automated model building, and one-click workflow execution.
- ModelArts aims to simplify AI development.
- ModelArts is a faster inclusive AI development platform.

- ModelArts covers all stages of AI development, including data processing, algorithm development, and model training and deployment. The underlying technologies of ModelArts support various heterogeneous computing resources, allowing developers to flexibly select and use resources. In addition, ModelArts supports popular open-source AI development frameworks such as TensorFlow, PyTorch, and MindSpore. ModelArts also allows you to use customized algorithm frameworks tailored to your needs.
- ModelArts is suitable for AI developers with varying levels of development experience. Service developers can use ExeML to quickly build AI applications without coding. Beginners can directly use built-in algorithms to build AI applications. AI engineers can use multiple development environments to quickly compile code for modeling and application development.

HUAWEI CLOUD ModelArts Advantages



HUAWEI CLOUD ModelArts Application Scenarios



Quiz

1. Which of the following are components of OpenStack?
   A. Nova
   B. Cinder
   C. Horizon
   D. Keystone
2. Cloud-native applications run on the cloud to take full advantage of the cloud.
   A. True
   B. False

- Answers:
  - ABCD
  - A

Summary

- In this chapter, we have learned the basic concepts and components of OpenStack, and the basic concepts of emerging technologies such as edge computing, blockchain, cloud native, and artificial intelligence. I believe you have a certain understanding of cloud computing and related basic technologies.
- At this point, the HCIA course of cloud computing is about to come to an end. In the subsequent certification courses, we will introduce Huawei HCS solution architecture, resource management, operation, and O&M management based on this course. Please look forward to it.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Acronyms and Abbreviations

- API: Application Programming Interface
- DevOps: Development and Operations, a set of processes, approaches, and systems

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI