

# 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

- Upon 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 technologies.

# Contents

## 1. IT Basics

- What Is IT?
- Challenges to Traditional IT
- IT Development Trend

## 2. About Cloud Computing

## 3. Mainstream Cloud Computing Vendors and Technologies

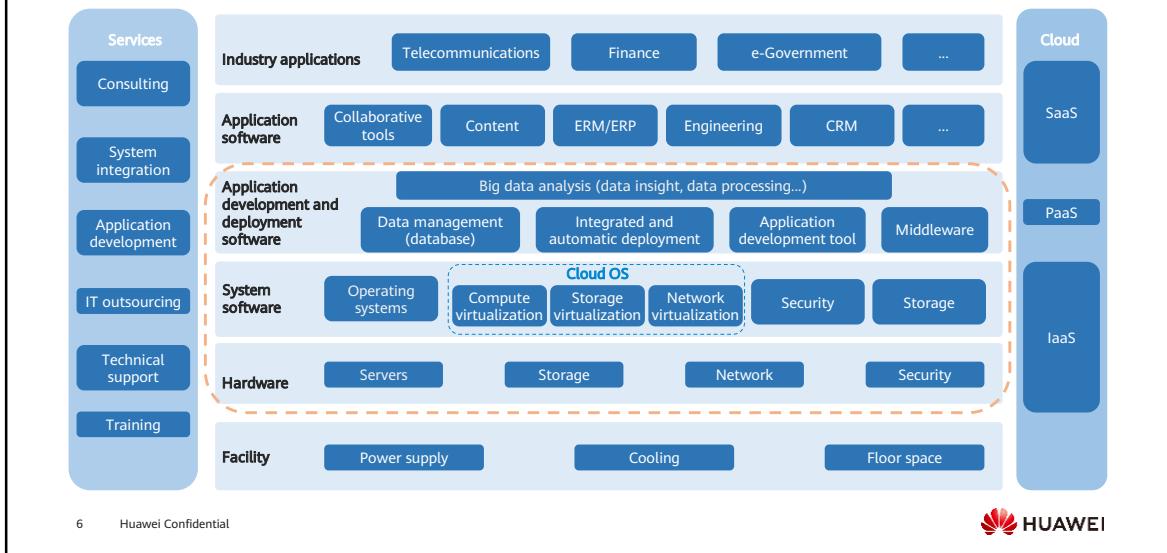
## IT All Around Us

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



- IT technologies 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

# Data Center - Based IT Architecture



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

## **1. IT Basics**

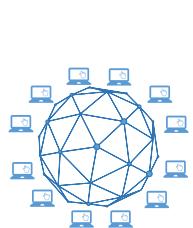
- What Is IT?
- Challenges to Traditional IT
- IT Development Trend

## 2. About Cloud Computing

## 3. Mainstream Cloud Computing Vendors and Technologies

## 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**

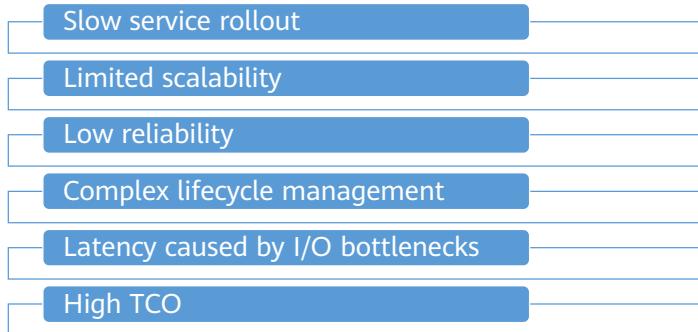


IoT  
Terminals running  
x86/Arm/DSP/MIPS/FPGA/...  
**IoT operating systems**

- In the PC era, computers are connected to each other through servers. Now, in the mobile era, we can access 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.



- 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

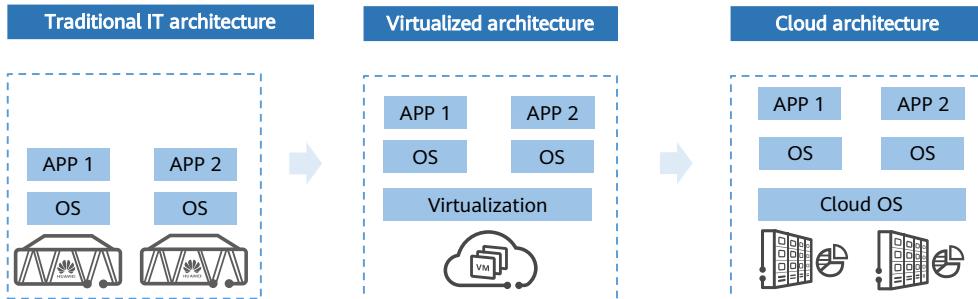
## **1. IT Basics**

- What Is IT?
- Challenges to Traditional IT
- **IT Development Trend**

## 2. About Cloud Computing

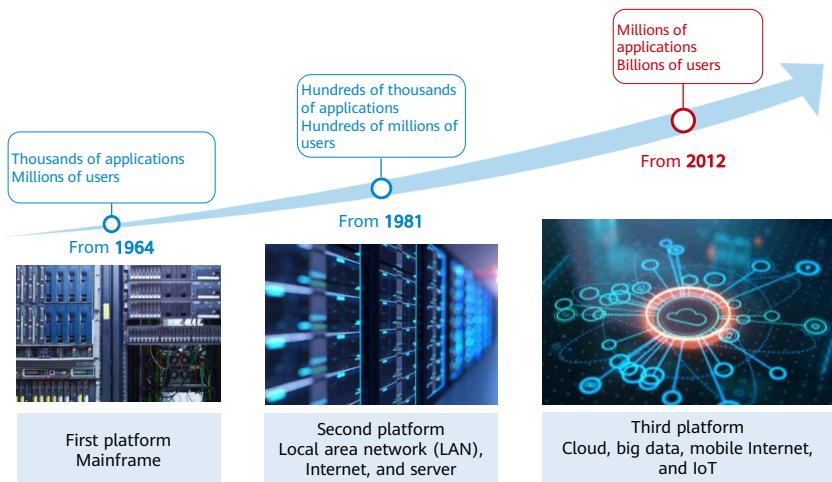
## 3. Mainstream Cloud Computing Vendors and Technologies

## 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.

## Cloud Computing Is Now the Preferred Choice for IT Enterprises



13     Huawei Confidential



- 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

1. IT Basics

## **2. About Cloud Computing**

- A Timeline of Computer History
  - A Timeline of Virtualization History
  - Definition of Cloud Computing
  - Development of Cloud Computing
  - Benefits of Cloud Computing
  - Cloud Computing Services and Deployment

3. Mainstream Cloud Computing Vendors and Technologies

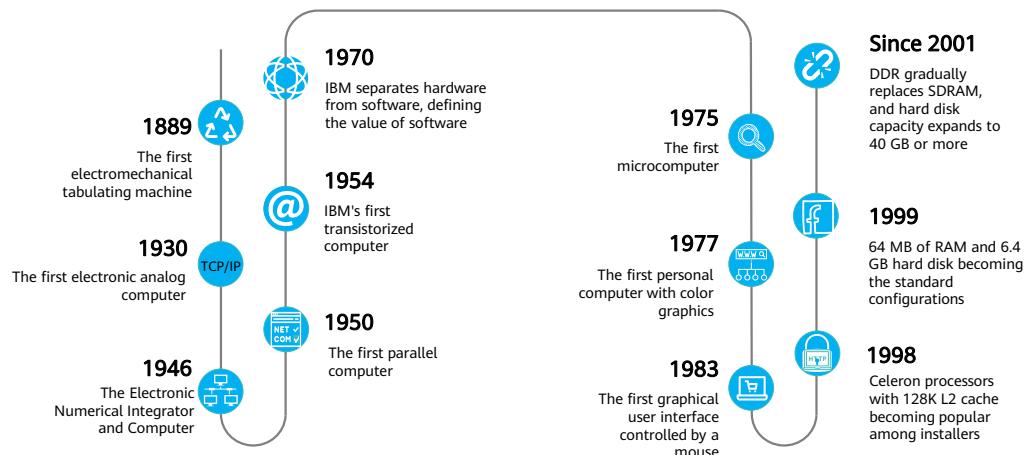
As what we have learnt from the previous slides, the third platform built on cloud computing has become the mainstream of the IT industry. Computer and virtualization technologies are the foundation of the third platform. Before we get into cloud computing, let's take a quick look at the evolution of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



# A Timeline of Computer History

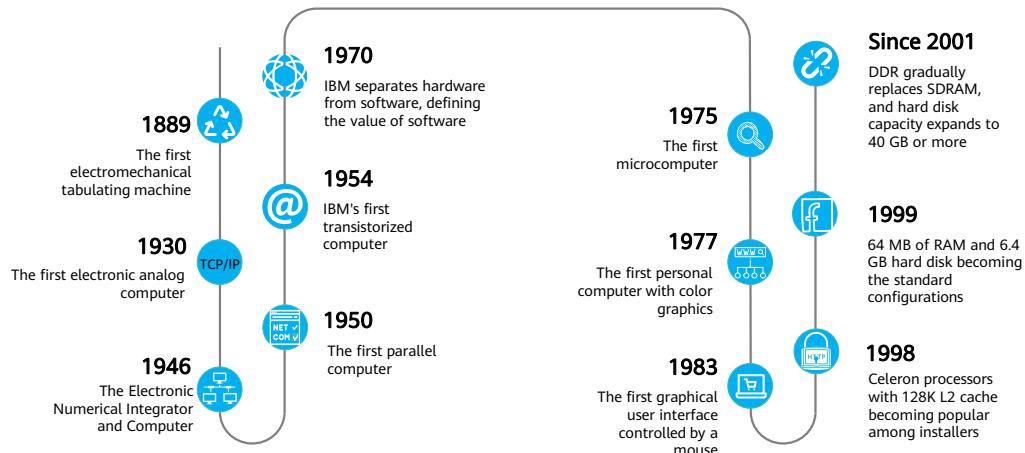


16      Huawei Confidential



- 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.

# A Timeline of Computer History



17      Huawei Confidential



- 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 64 MB of RAM and 15-inch displays became standard configurations.
- In 1999, Pentium III CPUs became a selling point for some computer manufacturers. The 64 MB of RAM and 6.4 GB 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 40 GB or more.

# Contents

1. IT Basics

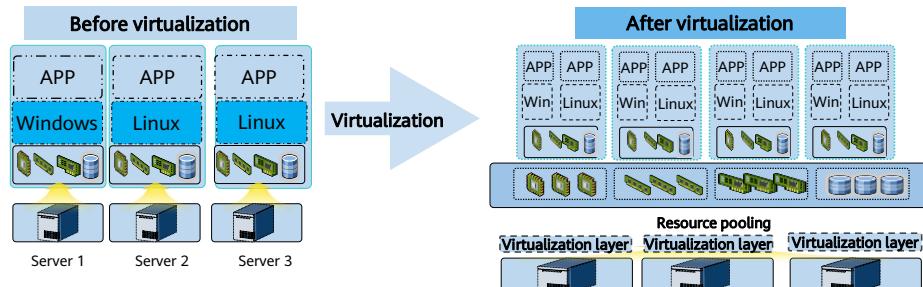
## **2. About Cloud Computing**

- A Timeline of Computer History
- **A Timeline of Virtualization History**
- Definition of Cloud Computing
- Development of Cloud Computing
- Benefits of Cloud Computing
- Cloud Computing Services and Deployment

3. Mainstream Cloud Computing Vendors and Technologies

## What Is Virtualization?

- Virtualization is the act of creating a virtual version of something, a logical representation of resources.

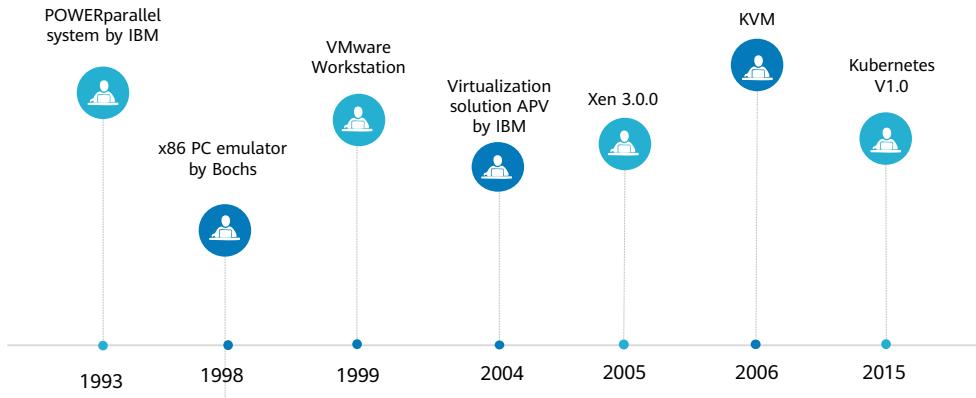


- IT resources are independent.
- The operating system (OS) is tightly coupled to the physical hardware.

- Resources are virtualized and placed in a shared resource pool.
- Resources are decoupled from the physical hardware, so the OS can allocate resources more flexibly.

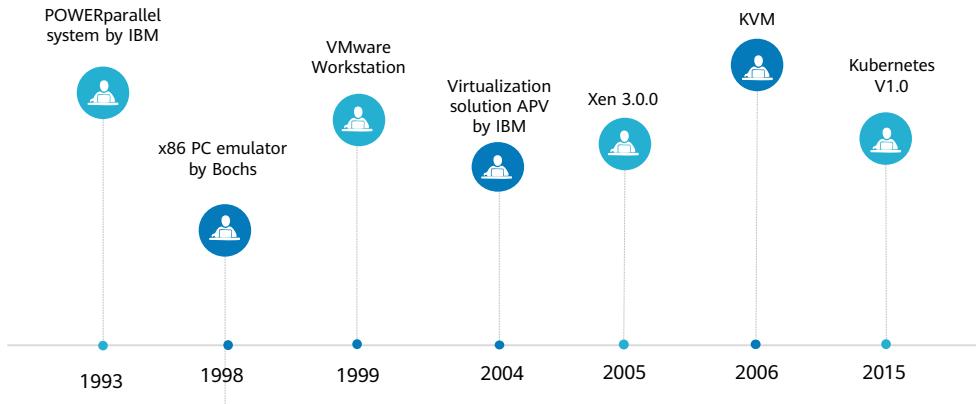
- Virtualization is the fundamental technology that powers cloud computing. Simply speaking, virtualization allows multiple virtual machines (VMs) to run on a physical server. The VMs share the CPU, memory, and I/O hardware resources on the physical server, but they are logically isolated from each other.
- 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.

## A Timeline of Virtualization History



- In 1993, IBM launched an upgradeable POWERparallel system, the first microprocessor-based supercomputer using RS/6000 technology.
- In 1998, Bochs, a x86 PC emulator was released.
- In 1998, VMware was founded. In 1999, the company launched its first product, VMware Workstation, the commercial virtualization software that allows to run multiple operating systems on a single physical server.
- In 1999, IBM first proposed the LPAR (logical partition) virtualization technology on AS/400.
- In 2000, Citrix released XenDesktop, a desktop virtualization product.
- In 2004, IBM announced the virtualization solution APV (Advanced Power Virtualization), which supports resource sharing. This solution was renamed PowerVM in 2008.
- In 2005, Xen 3.0.0 was released as the first hypervisor with Intel® VT-x support. Xen 3.0.0 can run on 32-bit servers.

## A Timeline of Virtualization History



21 Huawei Confidential



- In 2006, Qumranet, an Israeli startup, officially announced Kernel-based Virtual Machine (KVM).
- 2006–present: cloud computing and big data era.
- In 2007, German company InnoTek developed VirtualBox, a virtualization software.
- In 2008, Linux Container (LXC) 0.1.0 was released to provide lightweight virtualization.
- In 2010, Red Hat released RHEL 6.0, removing Xen and leaving KVM as the only bundled virtualization option.
- In 2015, Kubernetes v1.0 was released, and the cloud native era started.
- In 2019, 12 national regulations for cloud computing were approved and officially released.

# Contents

1. IT Basics

## **2. About Cloud Computing**

- A Timeline of Computer History
- A Timeline of Virtualization History
- **Definition of Cloud Computing**
- Development of Cloud Computing
- Benefits of Cloud Computing
- Cloud Computing Services and Deployment

3. Mainstream Cloud Computing Vendors and Technologies

In the previous two chapters, we have learned about the development of computers and virtualization technology. Now, let's see what cloud computing is.

# 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.



- 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

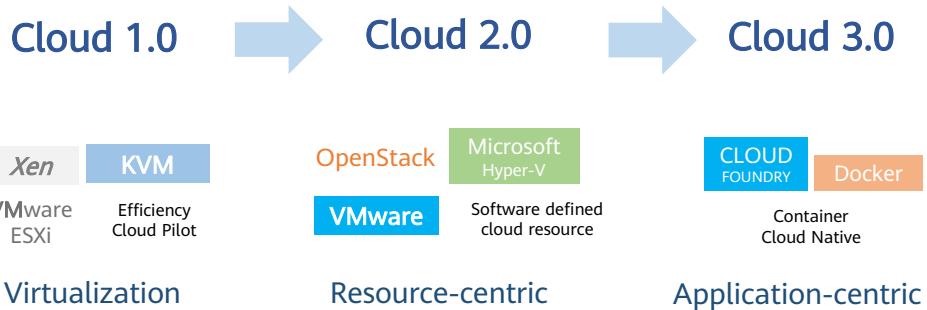
1. IT Basics

## **2. About Cloud Computing**

- A Timeline of Computer History
- A Timeline of Virtualization History
- Definition of Cloud Computing
- **Development of Cloud Computing**
- Benefits of Cloud Computing
- Cloud Computing Services and Deployment

3. Mainstream Cloud Computing Vendors and Technologies

## Development of Cloud Computing



- Looking back on the history of cloud computing, Cloud 1.0 is out of date. Some enterprises adopt Cloud 2.0 for commercial use and are considering expanding the scale and evolving to Cloud 3.0. The other enterprises are evolving from Cloud 1.0 to 2.0, and are even evaluating and implementing the evolution from Cloud 2.0 to 3.0.
- Cloud 1.0: virtualization for higher resource utilization
- Cloud 2.0: resource-centric for cloud-based infrastructure, as well as standardized and automated services
- Cloud 3.0: application-centric for cloud-based applications, agile application development, and easier lifecycle management

# Contents

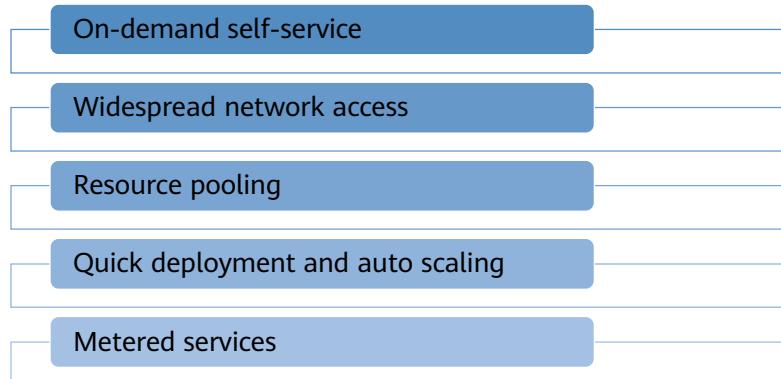
1. IT Basics

## **2. About Cloud Computing**

- A Timeline of Computer History
- A Timeline of Virtualization History
- Definition of Cloud Computing
- Cloud computing development process
- **Benefits of Cloud Computing**
- Cloud Computing Services and Deployment

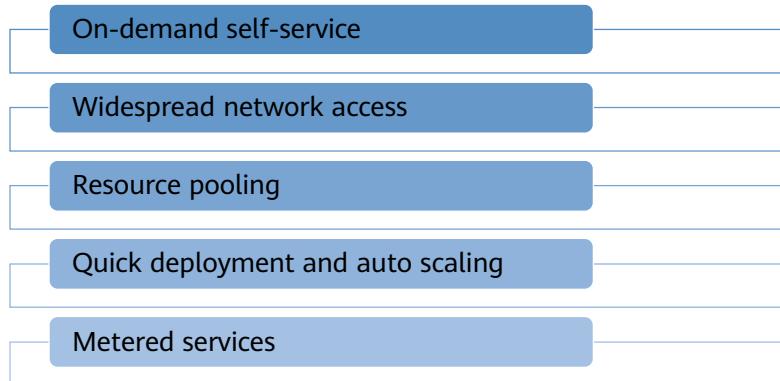
3. Mainstream Cloud Computing Vendors and Technologies

## Benefits of Cloud Computing



- 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 benefits:
  - 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.

## Benefits of Cloud Computing



- 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

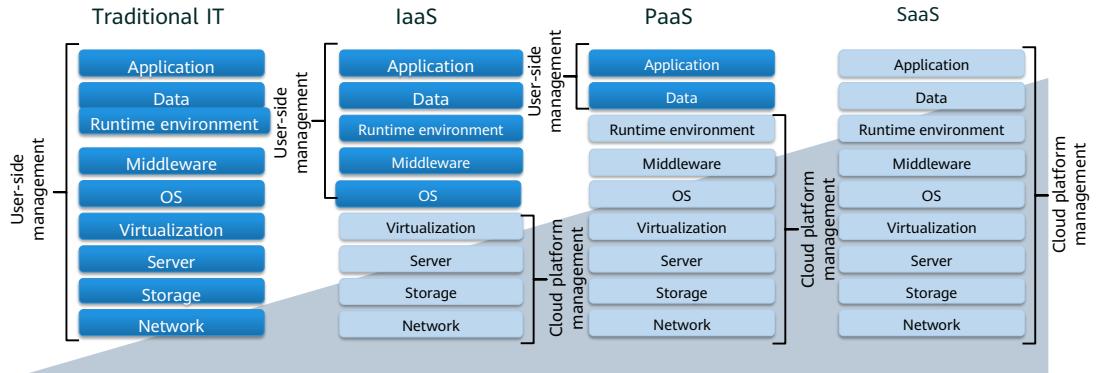
1. IT Basics

## **2. About Cloud Computing**

- A Timeline of Computer History
- A Timeline of Virtualization History
- Definition of Cloud Computing
- Cloud computing development process
- Benefits of Cloud Computing
- **Cloud Computing Services and Deployment**

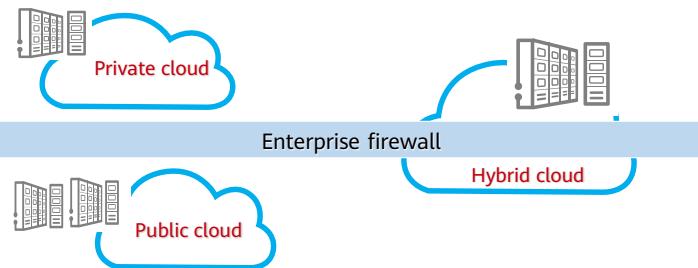
3. Mainstream Cloud Computing Vendors and Technologies

# Service Models for Cloud Computing



- 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.
- 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.

- Private cloud is a cloud infrastructure operated solely for a single organization. All data of the private cloud is kept within the organization's data center. Attempts to access such data will be controlled by ingress firewalls deployed for the data center, offering maximum data protection.
- Public cloud service provider owns and operates the cloud infrastructure and provides cloud services open to the public or enterprise customers. This model gives users access to convenient, on-demand IT services, comparable to how they would access utilities like water and electricity.
- A hybrid cloud is a combination of a public cloud and a private cloud or on-premises resources, that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Users can migrate workloads across these cloud environments as needed.

# Contents

1. IT Basics
2. About Cloud Computing
- 3. Mainstream Cloud Computing Vendors and Technologies**
  - AWS
  - VMware
  - Huawei Cloud

## AWS

Amazon Web Services (AWS) provides users with a set of cloud computing services, including scalable computing, storage, database, and applications, helping enterprises reduce IT investment and maintenance costs.



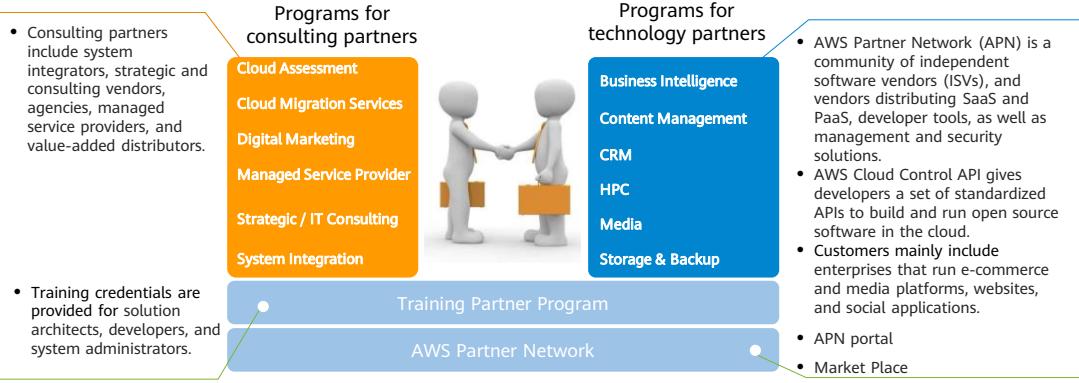
35      Huawei Confidential



AWS provides a complete set of infrastructure and application services, enabling users to run almost all applications on the cloud, including enterprise applications, big data projects, social games, and mobile applications.

# Extensive Partner Ecosystem

AWS partners can get support through a set of programs, including VMware Cloud on AWS, Distribution Program for Resellers, Managed Service Provider (MSP) Program, SaaS Factory Program, Competency Program, Public Sector Program, Marketplace Channel Programs.



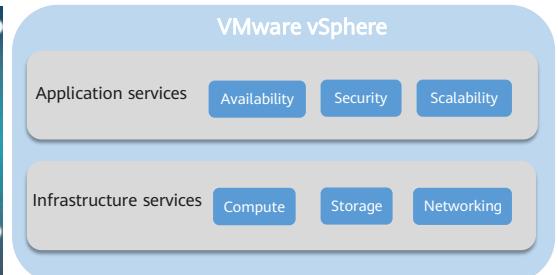
- Partner Ecosystem: AWS launched eight new partner programs for government and finance sectors.
- VMware on AWS enables partners to deploy and run VMware software on AWS.
- AWS service value:
  - Low price
  - More usage
  - Infrastructure expansion
  - Economies of scale
  - Technological innovation and ecosystem construction

# Contents

1. IT Basics
2. About Cloud Computing
- 3. Mainstream Cloud Computing Vendors and Technologies**
  - AWS
  - VMware
  - Huawei Cloud

## VMware

- VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation through enterprise control.
- VMware vSphere helps you run, manage, connect and secure your applications in a common operating environment across its hybrid clouds and cloud native public clouds.



- In 1998, VMware was founded. One year later, the company launched the commercial virtualization software VMware Workstation that can run smoothly on the x86 platform, marking its first step forward towards virtualization. In 2009, VMware launched VMware vSphere, the industry's first cloud operating system, and then launched the vCloud plan to build new cloud services.
- VMware delivers private, public, and hybrid cloud solutions designed for specified service requirements.
- VMware offers hybrid cloud products and services built based on the software-defined data center that brings together virtualized compute, storage, and networking.
- VMware Cloud Foundation provides integrated cloud native infrastructure, making it easy to run enterprise applications in private environment.
- For details about the VMware hybrid cloud solution, visit [https://www.vmware.com/hk/cloud-solutions/hybrid-cloud.html?src=WWW\\_HK\\_HPS2\\_Multi-Cloud\\_SiteLink](https://www.vmware.com/hk/cloud-solutions/hybrid-cloud.html?src=WWW_HK_HPS2_Multi-Cloud_SiteLink).

## VMware

Since its inception in 1998, VMware has been dedicated to providing customers with the flexibility and diversity required for building the future through disruptive technologies such as edge computing, artificial intelligence, blockchain, machine learning, and Kubernetes.



Digital workspace



Cloud environment



Application modernization



Telco cloud

- Application modernization: Modernize applications to accelerate digital innovation.
- Cloud environment: Build, run, manage, connect, and secure all applications on any cloud.
- Telco cloud: Build, run, manage, connect, and secure all applications on any cloud.
- Digital workspace: Enable any employees to work from anywhere, anytime with seamless employee experiences.

# Contents

1. IT Basics
2. About Cloud Computing
- 3. Mainstream Cloud Computing Vendors and Technologies**
  - AWS
  - VMware
  - Huawei Cloud

# Huawei Cloud

Official website: <https://www.huaweicloud.com/intl/en-us/>

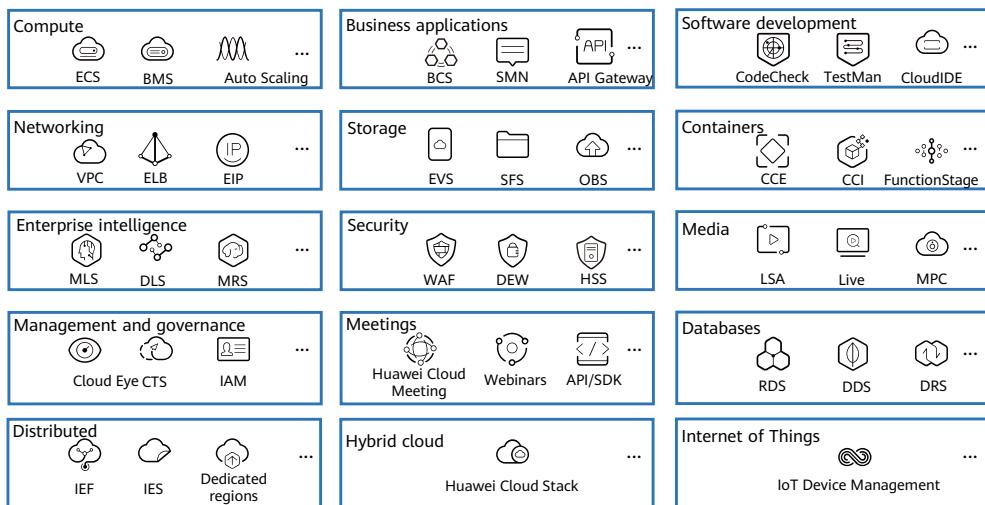
The screenshot shows the Huawei Cloud homepage. At the top, there's a navigation bar with links for Activities, Products, Solutions, Pricing, Documentation, Marketplace, Partners, Support, and About Us. A search bar is also present. Below the navigation, a large banner features the text "On-premises to On-cloud" and "Free cloud resources and professional migration services". It includes a "Learn More" button and a 3D illustration of a modern office environment transitioning into a cloud infrastructure setup. Below this, four promotional sections are displayed: "Free Packages" (30+ cloud services for free), "Go-China Solution" (Jump-start your business journey in China), "\$0.9 Intro Packages" (Start your cloud journey), and "Developer Forum" (Knowledge Sharing & Tech Communication). A footer section at the bottom of the page reads "Innovative, Trustworthy, and Secure Products and Services" followed by the text "Leverage Huawei's over 30 years of technical expertise to protect your applications and data".

41      Huawei Confidential



- Huawei Cloud is a public cloud service brand that leverages Huawei's more than 30 years of expertise in the ICT field to provide innovative, secure, and cost-effective cloud services.
- Huawei Cloud video:  
<http://3ms.huawei.com/documents/docinfo/524738282517131264>.

## 200+ Huawei Cloud Services



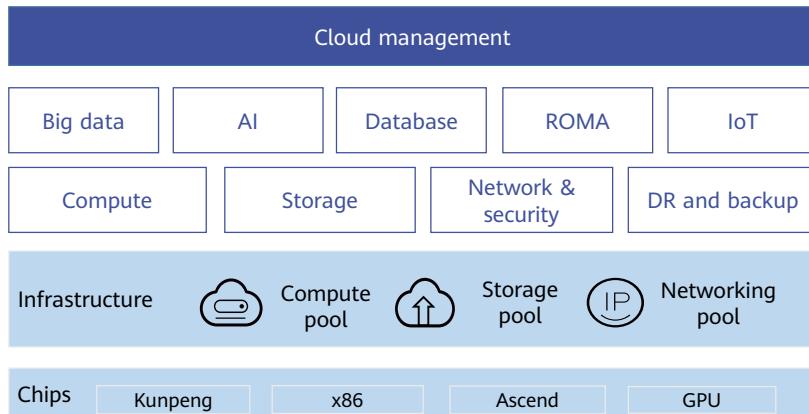
42      Huawei Confidential



Huawei Cloud has continuously upgraded its full-stack cloud native technologies. So far, they have launched more than 220 cloud services and more than 210 solutions.

# Huawei Cloud Stack

Huawei Cloud Stack is cloud infrastructure deployed at the on-premises data centers of government and enterprise customers.



- Huawei Cloud Stack combines the advantages of private cloud and public cloud, allowing you to quickly launch innovative services like you always do on the public cloud and to manage your resources like you always do on the private cloud. Huawei Cloud Stack can adjust to your organizational structure and business processes, serving you as a single cloud.
- Huawei Cloud Stack is ideal for medium- and large-sized enterprises that require local data storage or physical isolation of devices.
- Huawei Cloud Stack can be used for cloud migration, cloud native transformation, big data analysis, AI applications, industry clouds, and city clouds.
- Advantages:
  - AI enablement, data enablement, and application enablement: on-premises deployment of public cloud services
  - Multi-level cloud management: matching the enterprise governance architecture, featuring cloud federation, multi-level architecture, and intelligent O&M
  - Cloud-edge collaboration: extending intelligence to the edge, featuring unified framework, out-of-the-box edges, and video AI/IoT access
  - Secure and reliable: leading functions and performance, featuring full-stack security, one cloud with two pools, and strong ecosystem

# Huawei Cloud Data Centers: Innovation Starting from Chips

AI processors	Intelligent NICs	Faster & smarter SSD	Chip-based root of trust
<b>Ascend</b> Ascend AI processor	<b>HI1822</b> Industry's first 100 Gbit/s iNIC	<b>HI1812E</b> 4th generation SSD controller	<b>DAEMON</b> Chip-based root of trust
<ul style="list-style-type: none"><li>• 16 to 512 TOPS series products</li><li>• Innovative DaVinci architecture</li><li>• Optimized AI instruction sets</li></ul>	<ul style="list-style-type: none"><li>• Programmable NICs that perform better than standard NICs</li><li>• Multi-protocol offloading, including VxLAN, RoC, and OVS</li><li>• 15 MPPS, 2.5 times higher than the industry average</li></ul>	<ul style="list-style-type: none"><li>• IOPS: ↑ 75%+</li><li>• Bandwidth: ↑ 60%</li><li>• Latency: ↓ about 15% (thanks to intelligent multi-streaming)</li></ul>	<ul style="list-style-type: none"><li>• Firmware security protection</li><li>• Strong ID security protection</li><li>• Trustworthiness management</li></ul>

44      Huawei Confidential



- Chips are the core and most difficult part of R&D in the IT industry, which requires long-term investment.
- Huawei has over 20 years of experience in chip R&D and is constantly innovating chips for the Cloud 2.0 era. We have launched a full series of chips for next-generation cloud data centers.
  - Compute chips: full series of AI processors
  - Network chips: Huawei's next-generation network chips Hi822 use the NP-like programmable architecture and support offloading of multiple protocols.
  - Storage chips: The fourth generation of storage chips improves the performance by over 75% and bandwidth by over 60%. Thanks to the intelligent multi-stream technology, the latency was decreased by about 15%.
  - Security chips: Huawei has built security and trustworthiness into chips. They provide comprehensive protection for firmware, identities, software systems, and data management.
- The three vendors provide cloud solutions featuring resource pooling, unified management, and on-demand self-service. They leverage virtualized computing, storage, and networking technologies to provide users with ultimate experience.

- In the subsequent courses, let's take a closer look at these technologies and dig deeper into the principles of cloud computing.

# 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.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



## Server Basics



# Foreword

- Servers are the foundation of all service platforms, including cloud computing platforms. But what is a server? What are the key technologies for servers? Let's find the answers in this course, and start our learning journey into cloud computing.

# Objectives

- Upon completion of this course, you will be familiar with servers':
  - Role and features
  - Types
  - Hardware components
  - Key technologies

# Contents

## 1. Introduction to Servers

- What Is a Server?
  - Server Development History
  - Server Types
  - Server Hardware

## 2. Key Server Technologies

# Server Definition and Features

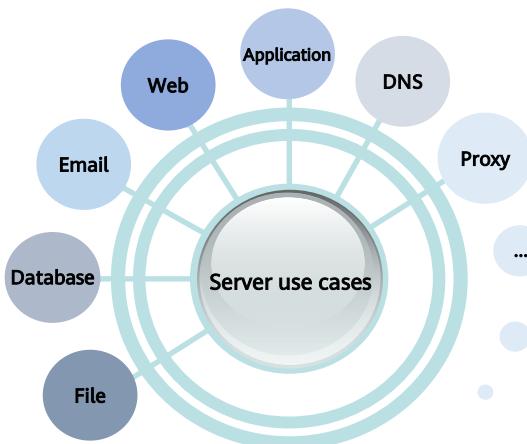
- Definition

- A server is a type of computer. It runs faster, carries more loads, and costs more than ordinary computers.
- A server provides services to users. There are file servers, database servers, and application servers.



- A server is a mainstream computing product developed in 1990s. It can provide network users with centralized computing, information release, and data management services. In addition, a server can share dedicated communication devices connected to it, such as drives, printers, and modems with network users.
- A server has the following features:
  - R: Reliability – the duration that the server operates consecutively
  - A: Availability – percentage of normal system uptime and use time
  - S: Scalability – including hardware expansion and operating system (OS) support capabilities
  - U: Usability – easy to maintain and restore server hardware and software
  - M: Manageability – monitoring and alarm reporting of server running status, and intelligent automatic fault processing

## Server Application Scenarios



6      Huawei Confidential



- Servers have been widely used in various fields, such as the telecom carrier, government, finance, education, enterprise, and e-commerce. Servers can provide users with the file, database, email, and web services.
- Server application deployment architecture:
  - C/S: short for Client/Server. In this architecture, the server program runs on the server, and the client software is installed on the client. The server and client perform different tasks. The client carries the front-end GUI and interaction operations of users, and the server processes the background service logic and request data. This greatly improves the communication speed and efficiency between the two ends. For example, you can install the vsftpd program on a file server and start the service. After you install the FileZilla or WinSCP client on your PC, you can upload and download files using the client.
  - B/S: short for Browser/Server. In this architecture, users only need to install a browser. The application logic is centralized on the server and middleware, which improves the data processing performance. For example, when accessing a website, we only need to enter the domain name of the website in the browser, for example, [www.huawei.com](http://www.huawei.com). Then we can see the web services provided by the background servers of the website. We do not need to care the background servers that provide services, such as the database service, proxy service, and cache service.

# Contents

## **1. Introduction to Servers**

- What Is a Server?
  - Server Development History
  - Server Types
  - Server Hardware

## **2. Key Server Technologies**

# Server Development History



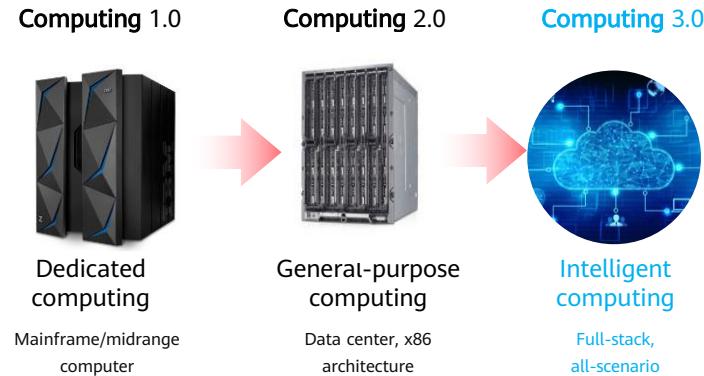
8      Huawei Confidential

 HUAWEI

- Mainframe phase
  - In the 1940s and 1950s, the first generation of vacuum tube computers emerged. The computer technology develops rapidly from vacuum tube computers, transistor computers, integrated circuit computers, to large-scale integrated circuit computers.
- Midrange computer phase
  - In the 1960s and 1970s, mainframes were scaled down for the first time to meet the information processing requirements of small- and medium-sized enterprises and institutions. The cost was acceptable.
- Microcomputer phase
  - In the 1970s and 1980s, mainframes were scaled down for the second time. Apple Inc. was founded in 1976, and launched Apple II in 1977. In 1981, IBM launched IBM-PC. After several generations of evolution, it occupied the personal computer market and made personal computers popular.
- x86 server era
  - In 1978, Intel launched the first-generation x86 architecture processor, 8086 microprocessor.
  - In 1993, Intel officially launched the Pentium series, which brought the x86 architecture processor to a new level of performance.
  - In 1995, Intel launched Pentium Pro, the x86 processor for servers, ushering in the x86 era. The standardization and openness of Pentium Pro also promoted the market development and laid a solid foundation for the cloud computing era.

- Cloud computing era
  - Since 2008, the concept of cloud computing has gradually become popular, and cloud computing becomes a popular word. Cloud computing is regarded as a revolutionary computing model because it enables the free flow of supercomputing capabilities through the Internet. Enterprises and individual users do not need to purchase expensive hardware. Instead, they can rent computing power through the Internet and pay only for the functions they need. Cloud computing allows users to obtain applications without the complexity of technologies and deployment. Cloud computing covers development, architecture, load balancing, and business models, and is the future model of the software industry.

## A Leap from Computing 1.0 to Computing 3.0



- The computing industry has developed for nearly half a century and continuously changed other industries. The computing industry itself is evolving.
- In the early mainframe and midrange computer era, dedicated computing is used, which is called computing 1.0. In the x86 era, under the leadership of Intel and driven by Moore's Law, computing has shifted from dedicated to general-purpose. A large number of data centers have emerged, which is called computing 2.0. With the rapid development of digitalization, the world is developing towards intelligent. Computing is not limited to data centers, but also enters the full-stack all-scenario (computing 3.0) era. This era is featured by intelligence, so it is also called intelligent computing.

# Contents

## 1. Introduction to Servers

- What Is a Server?
- Server Development History
- Server Types
- Server Hardware

## 2. Key Server Technologies

## Server Classification - Hardware Form

Server Category					
	Mainframe	Midrange computer	Tower server	Blade server	Rack server
Hardware form					

- **Tower server:**

- Some tower servers use a chassis roughly the same size as an ordinary vertical computer, while others use a large-capacity chassis, like a large cabinet.

- **Rack server:**

- The appearance of a rack server is different from that of a computer, but is similar to that of a switch. The specifications of a rack server include 1 U (1 U = 1.75 inches), 2 U, and 4 U. A rack server is installed in a standard 19-inch cabinet. Most of the servers in this structure are functional servers. A rack server is usually small in size. Multiple servers can be placed in a cabinet at the same time to obtain a higher processing capability.

For applications that require large data storage space, external extended storage devices can be used. DL series servers are suitable for enterprise data centers and environments with multiple applications. For mission-critical applications, DL series servers are preferred.

- **Blade server:**
  - Each blade server is a plugboard equipped with processors, memory modules, hard drives, and related components. Due to the special architecture, blade servers require dedicated chassis. Generally, a chassis can hold several to dozens of blade servers, suitable for scenarios such as high-performance computing, front-end servers running multiple applications, and backend central databases.
- For details about mainframes and midrange computers, see the preceding description.

## Server Classification - Service Scale

Server Category				
	Entry-level server	Work group server	Department-level server	Enterprise-level server
Service scale	Similar to a PC server	Low-end server that provides small-scale services (about 50 clients)	Mid-range server that serves about 100 clients	High-end server that is accessed by hundreds of clients

# Contents

## 1. Introduction to Servers

- What Is a Server?
- Server Development History
- Server Types
- Server Hardware

## 2. Key Server Technologies

# Contents

## **Server Hardware**

- **Hardware Structure**
  - CPU
  - Memory
  - Drive
  - RAID Controller Card
  - NIC
  - PSU and Fan Module

## Hardware Structure

- Huawei TaiShan 200 server



- 1 Chassis
- 2 Motherboard
- 3 Memory
- 4 CPU
- 5 CPU heat sink
- 6 Power supply unit (PSU)
- 7 Fan
- 8 Drive
- 9 Air duct

- TaiShan 200 Server User Guide
- 3D model display for a Huawei TaiShan 200 server: <https://support-it.huawei.com/server-3d/res/server/taishan2280e/index.html?lang=en>

# Contents

## Server Hardware

- Hardware Structure
- CPU
  - Memory
  - Drive
  - RAID Controller Card
  - NIC
  - PSU and Fan Module

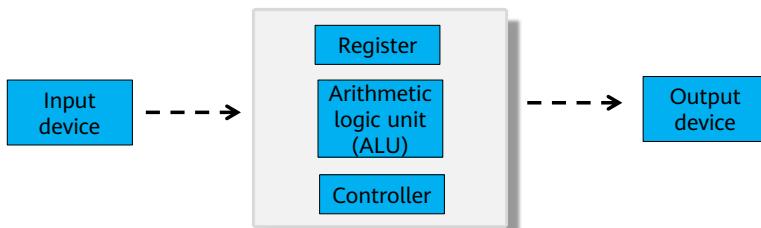
# CPU Definition and Components

- Definition

- The Central Processing Unit (CPU) is the computing and control core of a computer.
- The CPU, internal storage, and input/output devices are key components of a computer.
- The CPU interprets computer instructions and processes computer software data.

- Components

- The CPU consists of a logic operation unit, a control unit, and a storage unit.



- The CPU is the core processing unit on a server, and a server is an important device on the network and needs to process a large number of access requests. Therefore, servers must have high throughput and robust stability, and support long-term running. Therefore, the CPU is the brain of a computer and is the primary indicator for measuring server performance.
- The computer controls the entire computer according to a pre-stored program, and the program refers to an instruction sequence that can implement a function. The controller is an organization that issues commands to various logic circuits according to the instructions. The controller is a command center of the computer, controls work of an entire CPU, and determines automation of a running process of the computer.
- The ALU is a part of a computer that performs a variety of arithmetic and logical operations. Basic operations of an ALU include arithmetic operations such as addition, subtraction, multiplication, and division, logical operations such as AND, OR, NOT, and XOR, and other operations such as shift, comparison, and transfer. The ALU is also called the arithmetic logic component.
- The register is used to temporarily store the data involved in operations and the operation results. It can receive, store, and output data.

# CPU Frequency

- Dominant frequency
  - The dominant frequency is also called clock speed. It indicates, in MHz or GHz, the frequency at which a CPU computes and processes data.
- External frequency
  - The external frequency is the reference frequency of a CPU, measured in MHz. The CPU external frequency determines the speed of the motherboard.
- Bus frequency
  - The bus frequency directly affects the speed of data exchange between a CPU and a dual in-line memory module (DIMM).
- Multiplication factor
  - The multiplication factor is the ratio of the dominant frequency to the external frequency.

# Contents

## Server Hardware

- Hardware Structure
- CPU
- Memory
- Drive
- RAID Controller Card
- NIC
- PSU and Fan Module

# Memory

- Definition
  - Storage is classified, by purpose, into main memory and external storage. Main memory, referred to as internal storage, is the storage space that the CPU can address.
  - Memory is used to temporarily store CPU operation data and the data exchanged with external storage devices such as hard drives.
  - Memory, one of important computer components, communicates with the CPU.
  - Memory consists of the memory chip, circuit card, and edge connector.



- Storage, an important computer component, is used to store programs and data. For computers, the memory function can be supported and normal working can be ensured only when the storage is available.
- As a main computer component, the memory is in opposition to the external storage. Programs, such as the Windows operating system, typing software, and game software, are usually installed on external storage devices such as drives. To use these programs, you must load them into the memory. Actually, the memory is used when we input a piece of text or play a game. Bookshelves and bookcases for putting books are just like the external storage, while the desk is like the memory. Generally, we store large volumes of data permanently in the external storage and store small volumes of data and a few programs temporarily in the memory.
- Memory, one of important computer components, communicates with the CPU. Memory performance has great impacts on computers because all computer programs operate in the memory. The memory consists of the memory chip, circuit card, and edge connector.
- DIMM slots and configuration principles:
  - DIMMs on the same server must be of the same model.
  - At least one DIMM must be configured in slots supported by CPU 1.
  - Optimal memory performance can be achieved if the processors in a server are configured with the same number of DIMMs and the DIMMs are evenly distributed among the memory channels. Unbalanced configuration impacts memory performance and is not recommended.

# Contents

## Server Hardware

- Hardware Structure
- CPU
- Memory
- Drive
  - RAID Controller Card
  - NIC
  - PSU and Fan Module

## Drive

- The drive is the most important storage device of a computer.
- The drive interface, connecting a drive to a host, is used to transmit data between the drive cache and the host memory. The drive interface type determines the connection speed between the drive and the computer, how quickly programs run, and overall system performance.

	SATA	SAS	NL-SAS	SSD
<b>Rotational speed (RPM)</b>	7,200	15,000/10,000	7,200	N/A
<b>Serial/Parallel</b>	Serial	Serial	Serial	Serial
<b>Capacity (TB)</b>	1 TB/2 TB/3 TB	0.6 TB/0.9 TB	2 TB/3 TB/4 TB	0.6 TB/0.8 TB/1.2 TB/1.6 TB
<b>MTBF (h)</b>	1,200,000	1,600,000	1,200,000	2,000,000
<b>Remarks</b>	Developed from ATA drives, SATA 3.0 supports data transfer up to 600 MB/s.  The annual failure rate of SATA drives is about 2%.	SAS drives are designed to meet high-performance enterprise requirements and are compatible with SATA drives. The transfer rate ranges from 3.0 Gbit/s to 6.0 Gbit/s, and can increase to 12.0 Gbit/s.  The annual failure rate of SAS drives is less than 2%.	An NL-SAS drive is an enterprise-level SATA drive with a SAS interface. It is used to implement tiered storage in a drive array, simplifying drive array design.  The annual failure rate of NL-SAS drives is about 2%.	A solid-state drive (SSD) is a hard drive housing a solid-state electronic storage chip array. An SSD consists of a control unit and a storage unit (flash or DRAM chip).  An SSD is the same as a common hard drive in terms of interface specifications and definition, function, usage, and product shape and size.

- MTBF: Mean Time Between Failures
- SATA and NL-SAS drives are cheaper, SAS drives are more expensive, and SSDs are the most expensive.

# Contents

## Server Hardware

- Hardware Structure
- CPU
- Memory
- Drive
- RAID Controller Card
- NIC
- PSU and Fan Module

## RAID Controller Card

- Also called the RAID card.
- Functions of the RAID controller card:
  - Combines multiple drives into a system managed by the array controller according to requirements.
  - Improves drive subsystem performance and reliability.



LSI SAS3108

26      Huawei Confidential



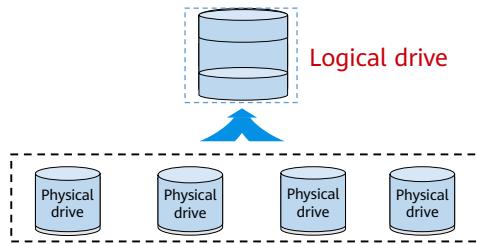
- LSI SAS3108 RAID Controller Card User Guide:  
<https://support.huawei.com/enterprise/en/doc/EDOC1100048773/653c6b1f>

# RAID

- **Definition**

- Redundant Array of Independent Disks (RAID) is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.

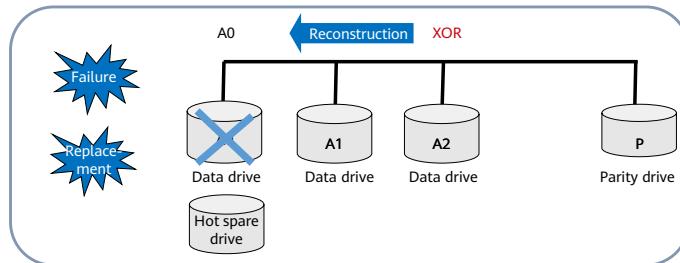
--Wikipedia



- For details about the working principles of RAID, see the course of storage basics.

## RAID Hot Spare and Reconstruction

- Hot spare definition
  - If a drive in a RAID array fails, a hot spare is used to automatically replace the failed drive to maintain the RAID array's redundancy and data continuity.
- Hot spare types
  - Global: The spare drive is shared by all RAID arrays in the system.
  - Dedicated: The spare drive is used only by a specific RAID array.

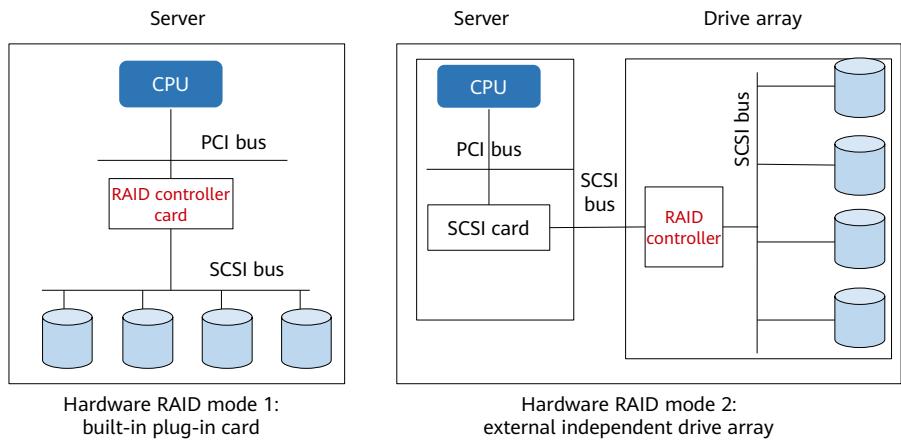


28      Huawei Confidential



- Data parity: Redundant data is used to detect and rectify data errors. The redundant data is usually calculated through Hamming check or XOR operations. Data parity can greatly improve the reliability, performance, and error tolerance of the drive arrays. However, the system needs to read data from multiple locations, calculate, and compare data during the parity process, which affects system performance.
- Generally, RAID cannot be used as an alternative to data backup. It cannot prevent data loss caused by non-drive faults, such as viruses, man-made damages, and accidental deletion. Data loss here refers to the loss of operating system, file system, volume manager, or application system data, not the RAID data loss. Therefore, data protection measures, such as data backup and disaster recovery, are necessary. They are complementary to RAID, and can ensure data security and prevent data loss at different layers.

## RAID Implementation - Hardware



- Hardware RAID is implemented using a hardware RAID adapter card.
- The hardware RAID can be a built-in or external RAID.
- A RAID controller card has a processor inside and can control the RAID storage subsystem independently from the host. The RAID controller card has its own independent processor and memory. It can calculate parity information and locate files, reducing the CPU computing time and improving the parallel data transmission speed.

## RAID Implementation - Software

- Definition
  - Software RAID implements RAID functions by installing software on the operating system.
- Characteristics
  - Software RAID does not require expensive RAID controller cards, reducing the cost.
  - RAID functions are performed by CPUs, requiring significant CPU resources, such as for large numbers of RAID 5 XOR operations.

- Software RAID does not provide the following functions:
  - Hot swap of drives
  - Drive hot spare
  - Remote array management
  - Support for bootable arrays
  - Array configuration on drives
  - S.M.A.R.T. for disks

## RAID Implementation - Mode Comparison

Mode	Software RAID	Built-in RAID	External RAID
<b>Characteristics</b>	All RAID functions are implemented by CPUs, resulting in high CPU usage and reduced system performance.	Built-in RAID improves performance by reducing host CPU usage caused by intensive RAID operations.	External RAID, connecting to a server through a standard controller, is independent of the operating system. All RAID functions are implemented by the microprocessor on the external RAID storage subsystem.
<b>Advantages</b>	<ul style="list-style-type: none"><li>▫ Low implementation cost</li><li>▫ Flexible configurations</li></ul>	<ul style="list-style-type: none"><li>▫ Data protection and high speed</li><li>▫ Better fault tolerance and performance than software RAID</li><li>▫ More cost-effective than external RAID</li><li>▫ Support for bootable arrays</li></ul>	<ul style="list-style-type: none"><li>▫ Provides ultra-large-capacity storage systems for high-end servers.</li><li>▫ Configures dual controllers to improve data throughput or provide shared storage for the two-node cluster.</li><li>▫ Supports hot swapping.</li><li>▫ Delivers better scalability.</li></ul>

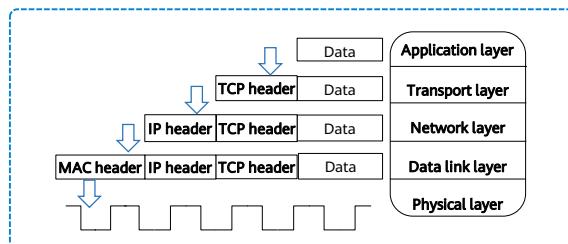
# Contents

## Server Hardware

- Hardware Structure
- CPU
- Memory
- Drive
- RAID Controller Card
- NIC
- PSU and Fan Module

# NIC Definition and Functions

- Definition
  - A network interface card (NIC or network adapter) is an indispensable part of a computer network system. An NIC enables a computer to access networks.
- Functions
  - Fixed network address
  - Data sending and receiving
  - Data encapsulation and decapsulation
  - Link management
  - Encoding and decoding



33      Huawei Confidential



- *TaiShan 200 DA121C Server Node Maintenance and Service Guide*

## Huawei Server NICs

- LOM card
  - It is embedded directly into the PCH chip on the server motherboard and cannot be replaced.
  - It provides two external GE electrical ports + two 10 Gbit/s optical/electrical ports. LOM cards do not occupy PCIe slots.
- PCIe card
  - Huawei has both self-developed and purchased PCIe cards. They can be installed in standard PCIe slots.
- FlexIO card
  - Huawei-developed, non-standard PCIe card, which can only be used with Huawei rack servers.
- Mezzanine card
  - Mezzanine cards are only used on the compute nodes of Huawei E9000 blade servers.



- PCI-Express (PCIe) is the third-generation I/O bus, or 3GIO, following ISA and PCI buses. This bus was proposed by Intel at the Intel Developer Forum (IDF) in 2001 and renamed PCI-Express after being certified and released by the PCI special interest group (SIG). Its main advantages are high data transmission rate, strong anti-interference, long transmission distance, and low power consumption.
- For Huawei servers, a PCIe card refers to the NIC in a PCIe slot.
- Visit the link below to learn how to install and remove a PCIe card:

<https://support.huawei.com/enterprise/en/doc/EDOC1100002169?section=o00d>

- *FusionServer Rack Server Product Documentation*
- *TaiShan 200 DA121C Server Node Maintenance and Service Guide*
- *E9000 Blade Server Product Documentation*

# Contents

## Server Hardware

- Hardware Structure
- CPU
- Memory
- Drive
- RAID Controller Card
- NIC
- PSU and Fan Module

## PSU and Fan Module

- Supplies power to servers.
- Supports redundancy to prevent power supply failures.
  - Fault warning and prevention
  - Pre-fault preventive maintenance
  - Non-disruptive server services
- The power supply subsystem includes:
  - Intelligent PSU
  - Fan module



PSU



Fan module

- Power supply redundancy modes:
  - 1+1: In this mode, each module provides 50% of the output power. When one module is removed, the other provides 100% of the output power.
  - 2+1: In this mode, three modules are required. Each module provides 1/3 of the output power. When one module is removed, each of the other two modules provides 50% of the output power.
- *E9000 Blade Server Product Documentation*

# Contents

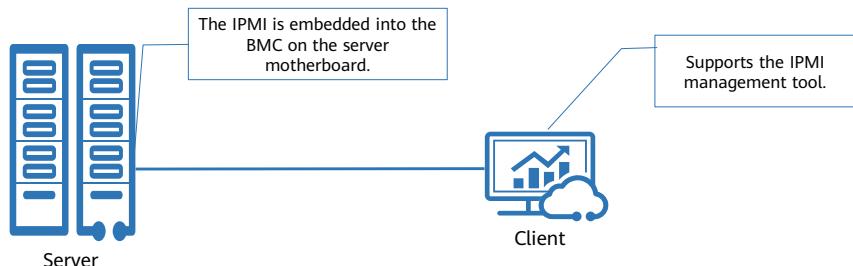
1. Server Introduction

## **2. Key Server Technologies**

- BMC
- BIOS

## What Is IPMI?

- Definition
  - The Intelligent Platform Management Interface (IPMI) is a set of open and standard hardware management interface specifications that defines specific methods for communication between embedded management subsystems.
  - IPMI information is exchanged using the baseboard management controller (BMC). Entry-level intelligent hardware, not the OS, handles management.



- The IPMI is an industrial specification used for peripherals in Intel-based enterprise systems. This interface specification was laid down by Intel, HP, NEC, Dell, and SuperMicro. Users can use the IPMI to monitor the physical health status of servers, such as the temperature, voltage, fan status, and power status. Moreover, the IPMI is a free specification. Users do not need to pay for this specification.
- IPMI development:
  - In 1998, Intel, DELL, HP, and NEC put forward the IPMI specification. The temperature and voltage can be remotely controlled through the network.
  - In 2001, the IPMI was upgraded from version 1.0 to version 1.5. The PCI Management Bus function was added.
  - In 2004, Intel released the IPMI 2.0 specification, which is compatible with the IPMI 1.0 and 1.5 specifications. Console Redirection is added. Servers can be remotely managed through ports, modems, and LANs. In addition, security, VLANs, and blade servers are supported.

## BMC

- Definition
  - The BMC complies with the IPMI specification. It collects, processes, and stores sensor signals, and monitors component operating status. It supplies the chassis management module with managed objects' hardware status and alarm information. The management module uses this information to manage the devices.



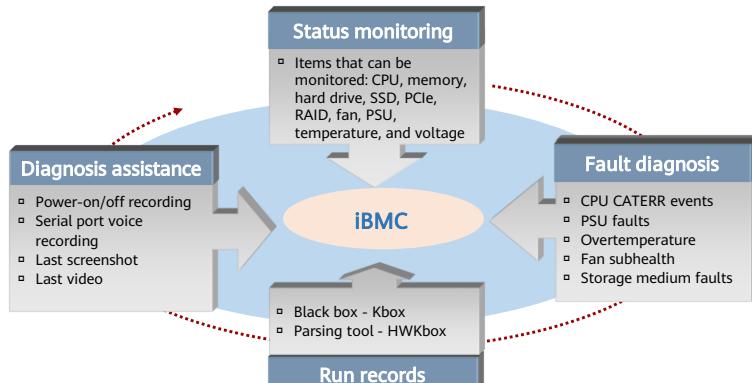
39      Huawei Confidential



- The BMC provides the following functions:
  - Remote control
  - Alarm management
  - Status check
  - Device information management
  - Heat dissipation control
  - Support for IPMItool
  - Web-based management
  - Centralized account management

## iBMC

- The Huawei Intelligent Baseboard Management Controller (iBMC) is a Huawei proprietary embedded server management system designed for the whole server lifecycle.



- The iBMC provides a series of management tools for hardware status monitoring, deployment, energy saving, and security, and standard interfaces to build a comprehensive server management ecosystem. The iBMC uses Huawei-developed management chip Hi1710 and multiple innovative technologies to implement refined server management.
- The iBMC provides a variety of user interfaces, such as the CLI, web-based user interface, IPMI integration interface, SNMP integration interface, and Redfish integration interface. All user interfaces adopt the authentication mechanism and high-security encryption algorithm to enhance access and transmission security.

# Contents

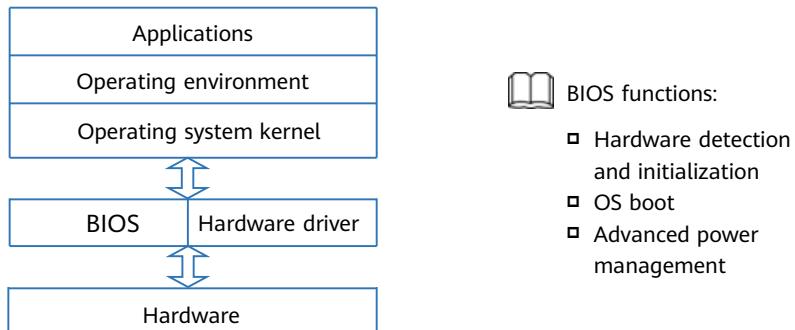
1. Introduction to Servers

## **2. Key Server Technologies**

- BMC
- BIOS

## BIOS

- Basic Input/Output System (BIOS)
- The BIOS is a system's foundation: a group of programs providing the most direct control of system hardware.



- The BIOS is a bridge between the system kernel and the hardware layer.
- Functions of the BIOS:
  - Software upgrade and loading
  - Basic OAM functions
  - Serial port management
  - Fault recovery
  - ECC management
  - Hardware diagnosis

# Quiz

1. Which of the following statements are true about the NICs of Huawei servers?
  - A. The LOM card is embedded into the PCH chip on the server motherboard and cannot be replaced.
  - B. Huawei-developed PCIe cards can be installed in standard PCIe slots.
  - C. A FlexIO card is integrated with the server panel for front-end service connection.
  - D. Mezzanine cards can be used with Huawei rack servers.
2. The BMC complies with the IPMI specification. It collects, processes, and stores sensor signals, and monitors component operating status.
  - A. True
  - B. False

- Answers:
  - AB
  - A

## Summary

- In this course, we have learned the basic concepts, development history, hardware components, and key technologies of servers. In the following course, we will learn about storage technologies. Stay tuned.

## Recommendations

- Huawei iLearning
  - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Support Case Library
  - <https://support.huawei.com/enterprise/en/knowledge?lang=en>

## Acronyms and Abbreviations

- BIOS: Basic Input/Output System
- BMC: Baseboard Management Controller
- B/S: browser/server architecture
- C/S: client/server architecture
- CPU: Central Processing Unit
- iBMC: Huawei Intelligent Baseboard Management Controller
- IPMI: Intelligent Platform Management Interface
- MTBF: Mean Time Between Failures
- NIC: Network Interface Card
- RAID: Redundant Array of Independent Disks



# 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.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



# Storage Technology Basics



# Foreword

- Data is the most important asset for every enterprise. This course describes how and where data is stored, and provides the key data storage technologies in cloud computing.

# Objectives

Upon completion of this course, you will be able to:

- Understand mainstream data storage modes and network topologies.
- Master RAID and Huawei RAID 2.0+ block virtualization technologies.
- Distinguish between centralized and distributed storage.
- Understand storage protocols and application scenarios.

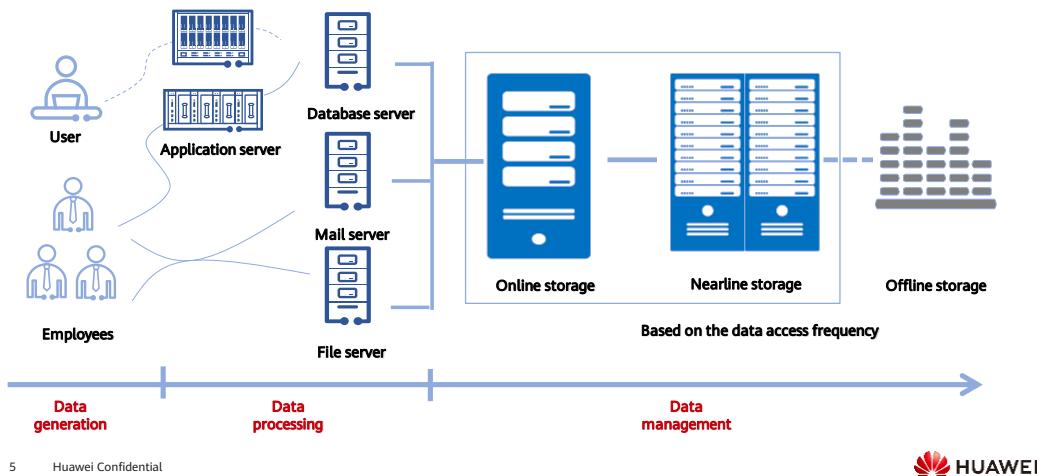
# Contents

## 1. Storage Basics

- Definition of Storage
- History of Storage
- Mainstream Disk Types
- Storage Networking Types
- Storage Forms

## 2. Key Storage Technologies

## What Is Storage?



- Storage in a narrow sense: CDs, DVDs, ZIP drives, tapes, and disks...
- Storage in a broad sense:
  - Storage hardware (disk arrays, controllers, disk enclosures, and tape libraries)
  - Storage software (backup software, management software, and value-added software such as snapshot and replication)
  - Storage networks (HBAs, Fibre Channel switches, as well as Fibre Channel and SAS cables)
  - Storage solutions (centralized storage, archiving, backup, and disaster recovery)

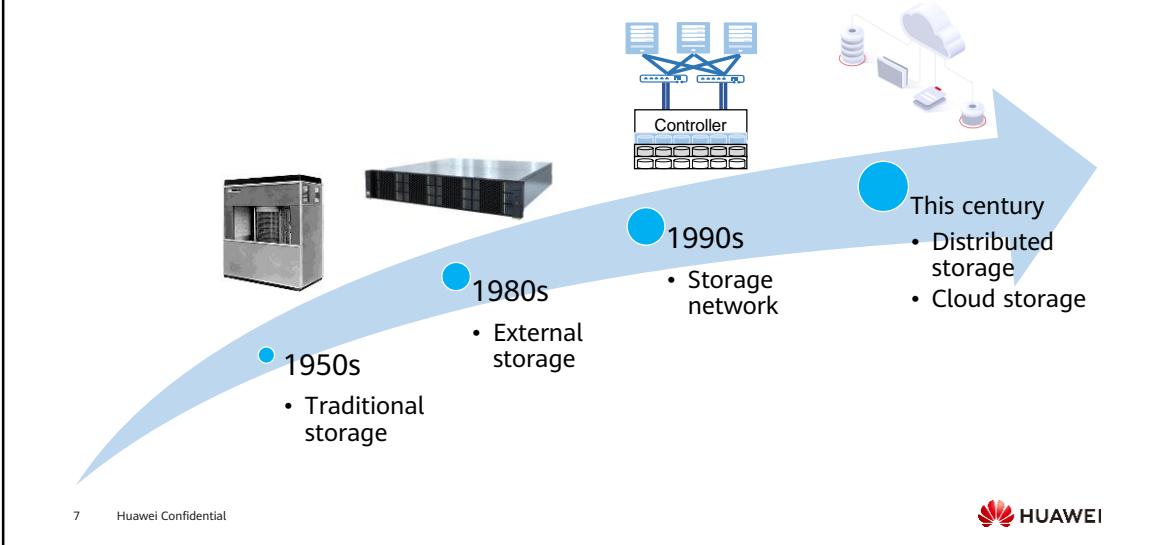
# Contents

## 1. Storage Basics

- Definition of Storage
- History of Storage
- Mainstream Disk Types
- Storage Networking Types
- Storage Forms

## 2. Key Storage Technologies

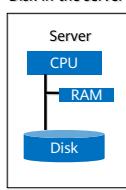
# History of Storage



- The storage architecture has gone through the following development phases: traditional storage, external storage, storage network, distributed storage, and cloud storage.
- Traditional storage refers to individual disks. In 1956, IBM invented the world's first mechanical hard drive that has fifty 24-inch platters and the total storage capacity of just 5 MB. It is about the size of two refrigerators and weighs more than a ton. It was used in the industrial field at that time and was independent of the mainframe.
- External storage refers to direct-attached storage. The earliest form of external storage is JBOD, which stands for Just a Bunch of Disks. JBOD is identified by the host as numerous independent disks. It provides large capacity but low security.
- A storage area network (SAN) is a typical storage network that transmits data mainly over a Fibre Channel network. Then, IP SANs emerge.
- Distributed storage uses general-purpose servers to build storage pools and is more suitable for cloud computing. This will be introduced later.

# Storage Development - from Server Attached Storage to Independent Storage Systems

Disk in the server

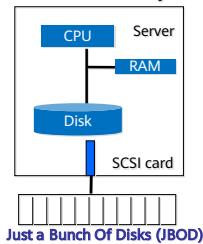


**Restrictions:**

- Disks become the system performance bottleneck.
- The number of disk slots is limited, thereby limiting capacity.
- Data is stored on a single disk, lowering data reliability.
- Storage space utilization is low.
- Data is scattered in local storage systems.



External disk array



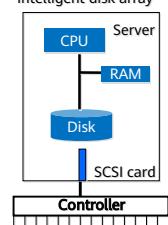
JBOD logically connects several physical disks to increase capacity.

**Problem solved:**

- The number of disk slots is limited, thereby limiting capacity.



Intelligent disk array



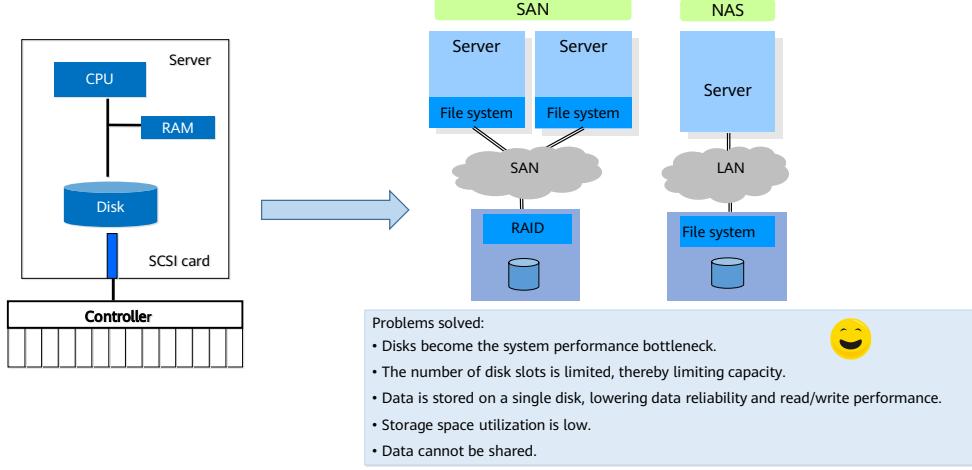
A controller provides the RAID function and large-capacity cache, and enables the disk array to have multiple functions for better read/write performance and data security.

**Problems solved:**

- Disks become the system performance bottleneck.
- The number of disk slots is limited, thereby limiting capacity.
- Data is stored on a single disk, lowering data reliability and read/write performance.



## Storage Development - from Independent Storage Systems to Network Shared Storage



- The direct connection between the controller and server resolves the problems caused by the limited disk slot quantities, single-disk storage, and poor disk interface performance.
- However, other problems remain, such as low storage space utilization, decentralized data management, and inconvenient data sharing. We will learn how the network shared storage in SAN or NAS mode solves these pain points.

# Contents

## 1. Storage Basics

- Definition of Storage
- History of Storage
- Mainstream Disk Types
  - Storage Networking Types
  - Storage Forms

## 2. Key Storage Technologies

## Introduction to Disks

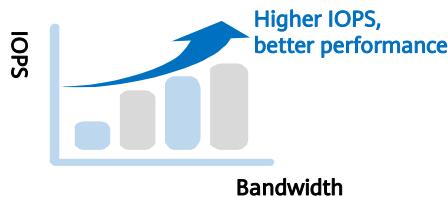
- Disks can be considered the most important storage device of a computer.
- A disk interface is a component used to connect a disk to a host. It transmits data between the disk cache and the host memory. The disk interface type determines the connection speed between the disk and the computer, the program running speed, and system performance.

	SATA	SAS	NL-SAS	SSD
<b>Rotational speed (rpm)</b>	7,200	15,000/10,000	7,200	N/A
<b>Serial/Parallel</b>	Serial	Serial	Serial	Serial
<b>Capacity (TB)</b>	1 TB/2 TB/3 TB	0.6 TB/0.9 TB	2 TB/3 TB/4 TB	0.6 TB/0.8 TB/1.2 TB/1.6 TB
<b>MTBF (h)</b>	1,200,000	1,600,000	1,200,000	2,000,000
<b>Remarks</b>	Being developed from ATA disks, SATA 3.0 supports up to 600 MB/s data transfer. The annual failure rate of SATA disks is about 2%.	SAS disks are designed to meet enterprises' high performance requirements, and are compatible with SATA disks. The transmission rate ranges from 3.0 Gbit/s to 6.0 Gbit/s, and will be increased to 12.0 Gbit/s. The annual failure rate of SAS disks is less than 2%.	NL-SAS disks are enterprise-class SATA drives with SAS interfaces. They are applicable to storage tiering in a disk array, which simplifies the design of the disk array. The annual failure rate of NL-SAS disks is about 2%.	Solid state disks (SSDs) are made up of solid-state electronic storage chip arrays. Each SSD consists of a control unit and a storage unit (DRAM or flash chip). SSDs are the same as the common disks in the regulations and definition of interfaces, functions, usage, as well as the exterior and size.

- MTBF: Mean Time Between Failure
- Increasing order of price: SATA and NL-SAS disks, SAS disks, and SSDs

## Disk Key Indicators

- Disk capacity
- Rotational speed (HDD only)
- Average access time
- Data transfer rate
- Input/Output operations per second (IOPS)



Disk Type	IOPS (4 KB random write)	Bandwidth (128 KB sequential read)
SATA	330	200 MB/s
SAS 10K	350	195 MB/s
SAS 15K	450	290 MB/s
SATA SSD	30,000 to 60,000	540 MB/s
SAS SSD	155,000	1000 MB/s
NVMe SSD	300,000	3500 MB/s

- **Disk capacity:** The capacity is measured in MB or GB. The factors that affect the disk capacity include the single platter capacity and the number of platters.
- **Rotational speed:** The rotational speed is the number of rotations made by disk platters per minute. The unit is rotation per minute (rpm). In most cases, the rotational speed of a disk reaches 5400 rpm or 7200 rpm. The disk that uses the SCSI interface reaches 10,000 rpm to 15,000 rpm.
- **Average access time** = Average seek time + Average wait time
- **Data transfer rate:** The data transfer rate of a disk is the speed at which the disk reads and writes data. It is measured in MB/s. The rate consists of the internal data transfer rate and the external data transfer rate.
- **Input/Output operations per second (IOPS):** indicates the number of input/output operations or read/write operations per second. It is a key indicator to measure disk performance. For applications with frequent random read/write operations, such as online transaction processing (OLTP), IOPS is a key indicator. Another key indicator is the data throughput, which indicates the amount of data that can be successfully transferred per unit time. For applications that require a large number of sequential read/write operations, such as video editing and video on demand (VoD) at TV stations, the throughput is more of a focus.

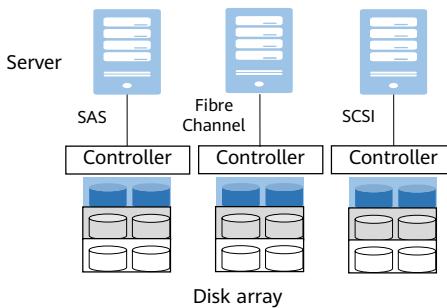
# Contents

## **1. Storage Basics**

- Definition of Storage
- History of Storage
- Mainstream Disk Types
- Storage Networking Types
- Storage Forms

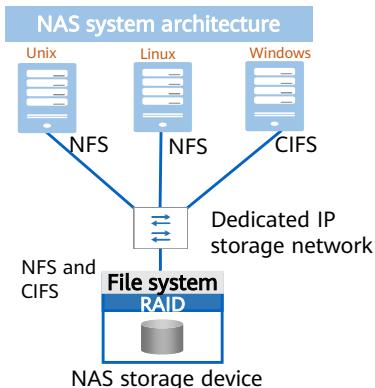
## **2. Key Storage Technologies**

## Introduction to DAS



- **Direct attached storage (DAS)**
- **Time:** 1970s
- **Background:** Data explosion drove up huge demand for storage. A simple storage architecture, DAS, was then introduced.
- **Connection mode:** **Fibre Channel, SCSI, or SAS**
- **Access mode:** The connection channels between DAS and server hosts often use SAS.
- **Link rate:** 3 Gbit/s, 6 Gbit/s, 12 Gbit/s
- **Provides functions, such as snapshot and backup.**

# Introduction to NAS (1)



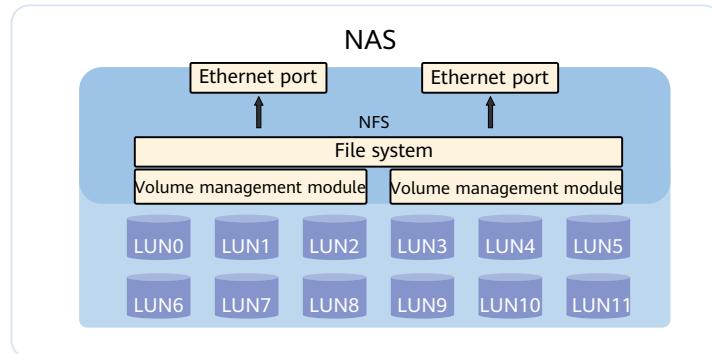
- **Network attached storage (NAS)**
- **Time:** early 1990s
- **Background:** Developing networks drove the need for [large-scale data sharing and exchange](#), leading to dedicated NAS storage devices.
- **Access mode:** Multiple front-end servers [share](#) space on back-end NAS storage devices using [CIFS](#) or [NFS Concurrent read and write operations](#) can be performed on the same directory or file.
- **The file system is on the back-end storage device.**

- **Network File System (NFS)** is an Internet standard protocol created by Sun Microsystems in 1984 for file sharing between systems on a local area network (LAN).
- Linux NFS clients support NFSv2 [RFC1094], NFSv3 [RFC1813], and NFSv4 [RFC3530]. NFSv2 that uses the User Datagram Protocol (UDP) is outdated due to its limited data access and transmission capabilities.
  - NFSv3, released in 1995, is widely used because Transmission Control Protocol (TCP) is added for transmission.
  - NFSv4, released in 2003, achieves better performance and security.
- NFS uses the Remote Procedure Call (RPC) protocol.
  - RPC provides a set of operations to achieve remote file access that are not restricted by machines, OSs, and lower-layer transmission protocols. It allows remote clients to access storage over a network like accessing a local file system.
  - The NFS client sends an RPC request to the NFS server. The server transfers the request to the local file access process, reads the local disk files on the server, and returns the files to the client.
- **Common Internet File System (CIFS)** is a network file system protocol used for sharing files and printers between machines on a network. CIFS is mainly used to

share network files between hosts running Windows.

## Introduction to NAS (2)

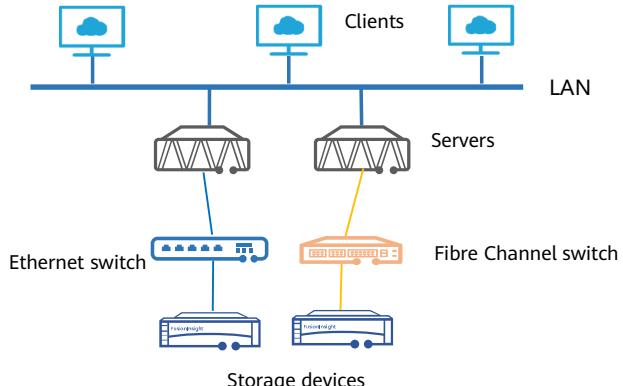
- NAS supports the centralized management of scattered and independent data, facilitating access to various hosts and application servers.



- NAS can serve as a network node and be directly connected to the network. In theory, NAS can support various network technologies and topologies. As Ethernet is the most popular network connection mode nowadays, we mainly discuss the NAS environment on the Ethernet.
- NAS supports multiple protocols (such as NFS and CIFS) and supports various OSs. Users can conveniently manage NAS devices by using Internet Explorer or Netscape on any work station.

## Introduction to SAN

- A storage area network (SAN) is a dedicated storage network that connects one or more network storage devices to servers.



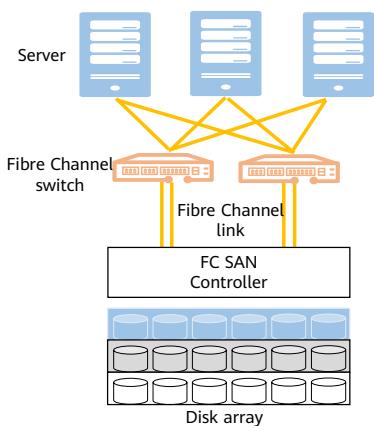
17      Huawei Confidential



- A SAN is a high-performance and dedicated storage network used between servers and storage resources. It is a back-end storage network independent from a LAN. The SAN adopts a scalable network topology for connecting servers and storage devices. The storage devices do not belong to any of the servers but can be shared by all the servers on the network.
- The SAN that uses Fibre Channel Protocol (FCP) to set up connections between servers and storage devices through Fibre Channel switches is called an FC SAN. Fibre Channel is especially suitable for SANs, because it supports long-distance and large-block transfer. The SAN mainly applies to high-end and enterprise-class storage applications, which have demanding requirements for performance, redundancy, and data availability.
- With the development of storage technologies, IP SANs based on TCP/IP also gains popularity. IP SANs feature high scalability, flexible interworking, long-distance data transmission, easy management and maintenance, and cost advantages.
- The major difference between NAS and SAN is that NAS provides a file operation and management system while SAN does not. SAN provides only data management, which is the layer below file management. SAN and NAS do not conflict with each other. They can coexist on the same network. However, NAS implements storage space management and resource sharing through a public interface, while SAN provides only a quick dedicate back-end channel for servers

to store data.

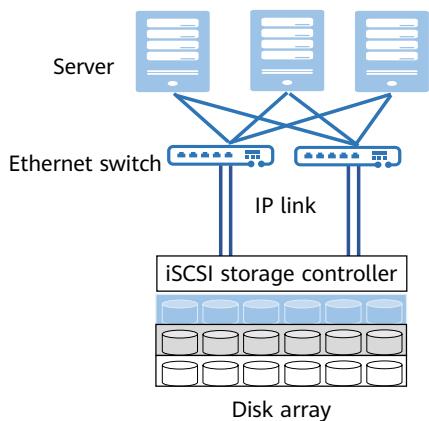
## Introduction to FC SAN



- **Fiber Channel storage area network (FC SAN)**
- **Time:** middle and late 1990s
- **Background:** To solve the poor scalability issue of DAS, storage devices was networked. [More than 100 servers](#) can be connected in a network.
- **Connection mode:** [Fibre Channel link; Fibre Channel switch](#)
- **Access mode:** The storage space on the back-end storage device can be divided into multiple [LUNs](#). Each LUN belongs to only one front-end server.
- **Link rate:** 2 Gbit/s, 4 Gbit/s, or 8 Gbit/s
- **Provides advanced data protection functions, such as snapshot and disaster recovery.**

- Fibre Channel (FC) is a standard data storage network used to transmit 100 Mbit/s to 4.25 Gbit/s signals over fiber or copper cables. It is a high-speed transport technology used to build SANs. Fibre Channel is primarily used for transporting SCSI traffic from servers to disk arrays, but it can also be used on networks carrying ATM and IP traffic.

## Introduction to IP SAN



- **IP storage area network (IP SAN)**
- **Time:** 2001
- **Background:** IP SAN is designed to solve the [price and management issues](#) of the FC SAN.
- **Connection mode:** [Ethernet link; Ethernet switch](#)
- **Access mode:** The storage space on the back-end storage device can be divided into multiple LUNs. Each LUN belongs to only one front-end server.
- **Link rate:** [1 Gbit/s, or 10 Gbit/s](#)
- The IP SAN provides advanced data protection functions, such as snapshot and disaster recovery.
- iSCSI is a mainstream choice because:
  - Mature IP network management tools and infrastructure can be used.
  - IP networks are widely used, which can reduce a large number of construction, management, and personnel costs.

- **Internet Small Computer System Interface (iSCSI)** is a storage technology based on the Internet and SCSI-3 protocol. It transmits the SCSI protocol, originally used only for local hosts, over the TCP/IP network to extend the connection distance. In the following course, we will learn about the protocol encapsulation, working principles, and application scenarios.

## Comparison Between Storage Networking Types

	DAS	NAS	SAN	
			FC SAN	IP SAN
Transmission mode	SCSI, Fibre Channel, and SAS	IP	Fibre Channel	IP
Data type	Block-level	File-level	Block-level	Block-level
Application scenario	Any	File servers	Database applications	Video security
Advantage	Easy to understand; robust compatibility	Easy to install; low cost	High scalability and performance; high availability	Strong scalability; low cost
Disadvantage	Difficult management; limited scalability; low storage space utilization	Low performance; inapplicable to some applications	Expensive and complex configuration; poor networking compatibility	Low performance

# Contents

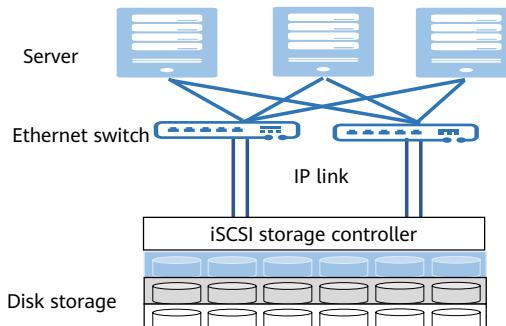
## **1. Storage Basics**

- Definition of Storage
- History of Storage
- Mainstream Disk Types
- Storage Networking Types
- Storage Forms

## **2. Key Storage Technologies**

## Centralized Storage

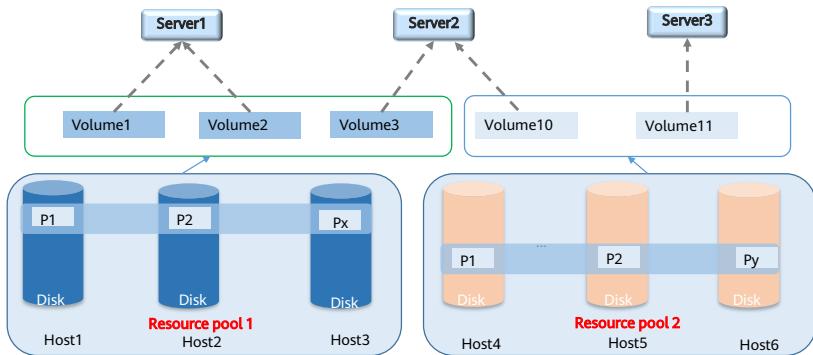
- A centralized storage system refers to one set of storage system consisting of multiple devices. Enterprises often deploy their storage devices on a centralized environment. For example, the Huawei storage system may need several cabinets to house devices. In terms of technical architectures, centralized storage is classified into SAN (including FC SAN and IP SAN) and NAS storage.
- Centralized storage has a simple deployment structure, which means you do not need to consider how to deploy multiple nodes for a service, or the distributed collaboration between multiple nodes.



- Disadvantages of centralized storage:
  - Isolated storage resources: Storage devices are connected to a limited number of servers through a dedicated network.
  - Scale-up by adding disk enclosures: The hardware controller performance (a single controller with disks) becomes a bottleneck.
  - Scale-out by connections between controllers: The hardware controller performance becomes a bottleneck.
  - No resource sharing: Storage devices and resources are provided by different vendors, and resources cannot be shared among devices. Storage pools are isolated in data centers.
  - Centralized metadata management: The system concurrency is limited by the metadata service performance. The metadata service becomes the performance bottleneck.
- How to solve the capacity expansion and performance bottleneck issues of traditional centralized storage?

## Distributed Storage

- A distributed storage system stores data on multiple independent devices. It adopts a scalable system architecture and enables multiple storage servers to share the storage load, improving scalability, reliability, availability, and access efficiency. As distributed storage is becoming more popular, some applications requiring high performance, such as databases of financial systems, also use distributed storage.

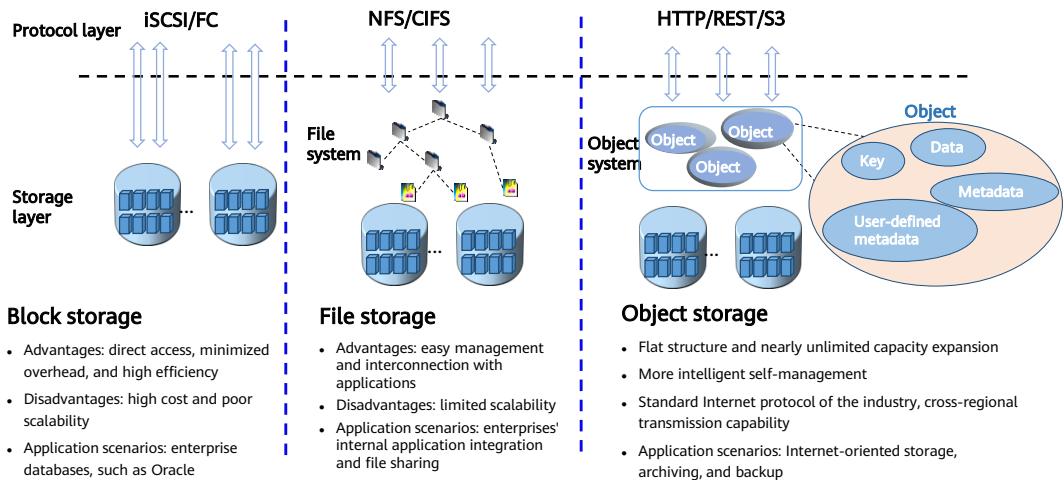


23 Huawei Confidential



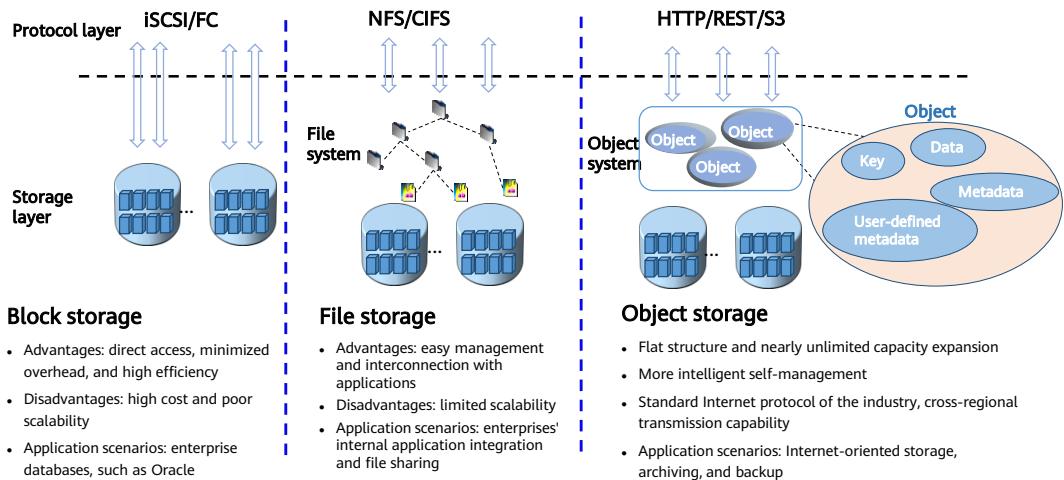
- Distributed storage uses software to simulate the functions of the original hardware controllers, avoiding the disadvantages of the hardware controllers.
- Resource pool: A resource pool is similar to a RAID group in SAN storage.

## Storage Service Type



- Users can access data in an object storage as fast as in a SAN storage and can share data as easy as in a NAS storage. Object storage has high reliability and secure data sharing between platforms. The following describes the comparison among the object storage, block storage, and file storage:
  - Block storage** directly accesses the storage layer, featuring fast speed, minimum overhead, and maximum efficiency. However, block storage has the high cost and poor scalability. Block storage employs iSCSI and Fibre Channel. Therefore, it is difficult to transmit data across networks. Block storage is applicable to enterprise databases, such as Oracle.
  - File storage** creates a file system on the basis of block storage. Data is organized in the directory-directory-file mode, facilitating data management. The objects operated by most application programs are files. Therefore, file storage enables easier interworking with application systems. File systems are restricted by directory trees. Therefore, a file system can be typically expanded to dozens of PB at most. The scalability is limited. File systems are applicable to application integration and file sharing in an enterprise.

## Storage Service Type



- Object storage creates the object management layer above block storage. Compared with the file system, the object system is flat with little expansion limitation. An object consists of a unique key, file, data (file), metadata, and user-defined metadata. An object contains self-management information. Therefore, object storage is more intelligent. Using compatible standard Internet protocol interfaces, object storage supports cross-region transmission. Object storage applies to storage scenarios for Internet services, and internal archiving and backup scenarios for enterprises.

# Contents

1. Storage Basics
2. Key Storage Technologies
  - RAID Technologies
  - Storage Protocol

## What Is RAID?

- Redundant Array of Independent Disks (RAID) combines multiple physical disks into one logical disk in different ways, improving read/write performance and data security.

- RAID levels based on combination methods

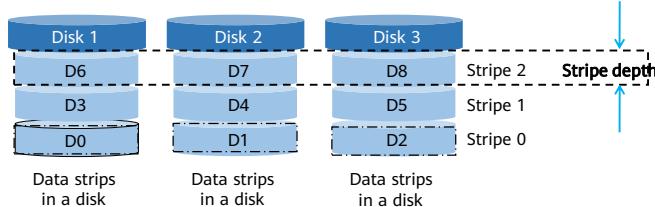
<b>RAID 0</b>	Data striping, no parity
<b>RAID 1</b>	Data mirroring, no parity
<b>RAID 3</b>	Data striping, with dedicated parity
<b>RAID 5</b>	Data striping, with distributed parity
<b>RAID 6</b>	Data striping, with double distributed parity

- RAID levels by using two different RAID modes

<b>RAID 0+1</b>	Create RAID 0 and then RAID 1, providing data striping and mirroring.
<b>RAID 10</b>	Similar to RAID 0+1. The difference is that RAID 1 is created before RAID 0.
<b>RAID 50</b>	Create RAID 5 and then RAID 0, effectively improving the performance of RAID 5.

## RAID Data Distribution

- Disk striping: Space in each disk is divided into multiple strips of a specific size. Written data is also divided into blocks based on the strip size.
- Strip: A strip consists of one or more consecutive sectors in a disk, and multiple strips form a stripe.
- Stripe: A stripe consists of strips of the same location or ID on multiple disks in the same array.

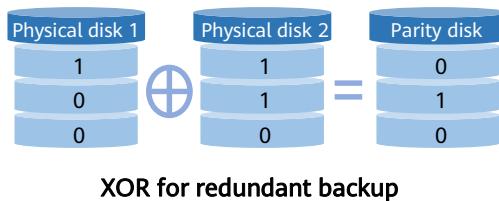


- Stripe width
  - Indicates the number of disks in an array for striping. For example, if a disk array consists of three member disks, the stripe width is 3.
- Stripe depth
  - Indicates the size of a stripe.

## RAID Data Protection

- 1. Mirroring: Data copies are stored on another redundant disk.
- 2. Parity check algorithm (XOR)
  - XOR is widely used in digital electronics and computer science.
  - XOR is a logical operation that outputs true only when inputs differ (one is true, the other is false).

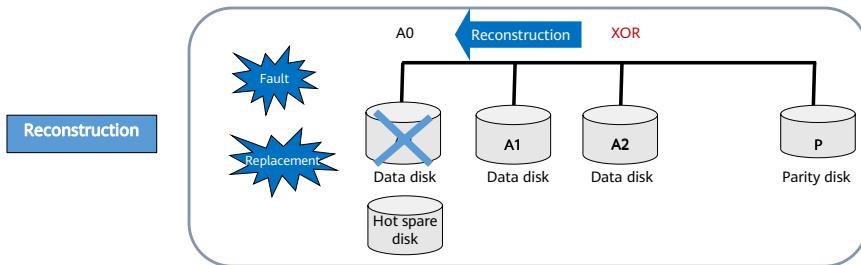
- $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$



- RAID generally protects data by the following methods:
  - Stores data copies on a redundant disk to improve reliability and read performance.
  - Uses the parity check algorithm. Parity data is additional information calculated using user data. For a RAID array that uses parity, an additional parity disk is required. The XOR (symbol:  $\oplus$ ) algorithm is used for parity.

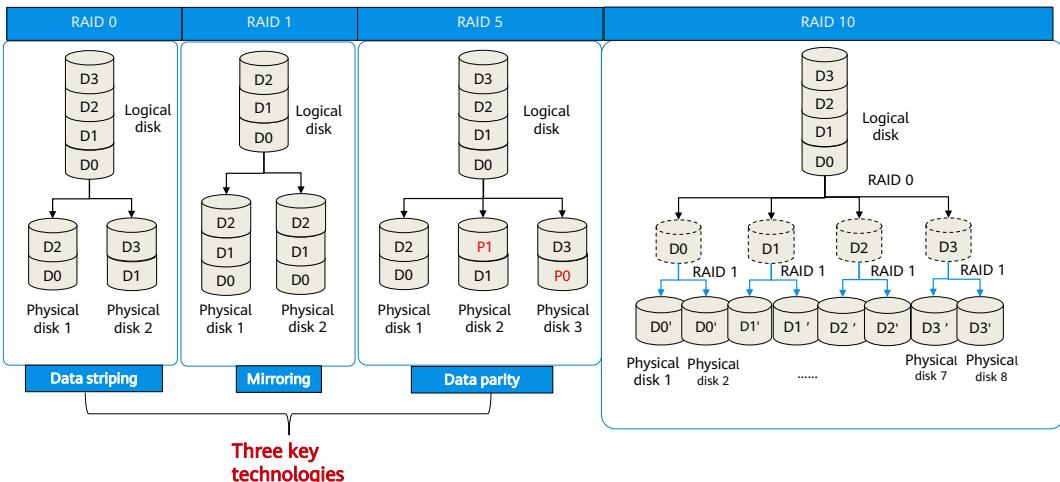
# RAID Hot Spare and Reconstruction

- Hot spare
  - If a disk in a redundant RAID group is faulty, a functional backup disk in the RAID group can automatically replace the faulty one to ensure RAID system redundancy.
- Hot spare can be classified into the following types:
  - Global: The spare disk is shared by all RAID groups in the system.
  - Dedicated: The spare disk is used only by a specific RAID group in the system.



- Data parity: Redundant data is used to detect and rectify data errors. The redundant data is usually calculated through Hamming check or XOR operations. Data parity can greatly improve the reliability, performance, and error tolerance of the disk arrays. However, the system needs to read data from multiple locations, calculate, and compare data during the parity process, which affects system performance.
- Generally, RAID cannot be used as an alternative to data backup. It cannot prevent data loss caused by non-disk faults, such as viruses, man-made damages, and accidental deletion. Data loss here refers to the loss of operating system, file system, volume manager, or application system data, not the RAID data loss. Therefore, data protection measures, such as data backup and disaster recovery, are necessary. They are complementary to RAID, and can ensure data security and prevent data loss at different layers.

## Common RAID Levels



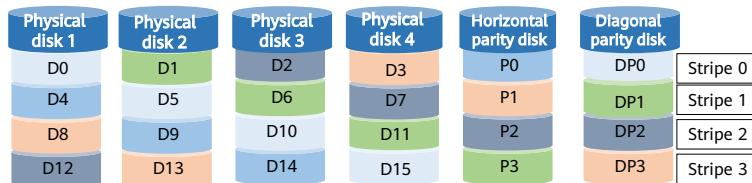
31      Huawei Confidential



- RAID 0 consists of striping without fault tolerance. Data of the RAID group is evenly distributed on all disks in stripe form.
- RAID 1, also called mirroring, can simultaneously write data into the primary disk and mirror disk.
- RAID 3 consists of striping with dedicated parity. Data is striped on data disks, and parity data is stored on a dedicated parity disk.
- RAID 5 is similar to RAID 3 except that parity information is evenly distributed among data disks. RAID member disks store both the data and the parity information, and data blocks and corresponding parity information are stored on different disks. RAID 5 is one of the most commonly used RAID levels.
- RAID 10 combines mirroring and striping. The first level is RAID 1 mirrored pairs, and the second level is RAID 0. RAID 10 is also a widely used RAID level.

## Working Principles of RAID 6 DP

- Double parity (DP): In addition to the horizontal XOR parity disk used in RAID 4, it adds another disk to store diagonal XOR parity data.
- P0 to P3 on the horizontal parity disk are the parity information of horizontal data on all data disks.
  - For example,  $P_0 = D_0 \text{ XOR } D_1 \text{ XOR } D_2 \text{ XOR } D_3$
- DP 0 to DP 3 in the diagonal parity disk represent the diagonal parity data for respective data disks and the horizontal parity disk.
  - For example,  $DP_0 = D_0 \text{ XOR } D_5 \text{ XOR } D_{10} \text{ XOR } D_{15}$



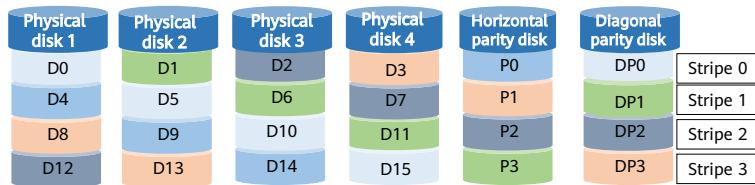
32 Huawei Confidential



- RAID 6 DP has two independent parity data blocks: horizontal parity data and diagonal parity data.
- Parity values in the horizontal parity disk are also called parity check values, which are obtained by performing the XOR operation on user data in the same stripe. As shown in the following figure, P0 is obtained by performing an XOR operation on D0, D1, D2, and D3 on a stripe 0, and P1 is obtained by performing an XOR operation on D4, D5, D6, and D7 on a stripe 1. Therefore,  $P_0 = D_0 \oplus D_1 \oplus D_2 \oplus D_3$ ,  $P_1 = D_4 \oplus D_5 \oplus D_6 \oplus D_7$ , and so on.
- The diagonal parity uses the diagonal XOR operation to obtain the row-diagonal parity data block. A process of selecting a data block is relatively complex. DP0 is obtained by performing an exclusive OR operation on D0 on a stripe 0 of a hard disk 1, D5 on a stripe 1 of a hard disk 2, D10 on a stripe 2 of a hard disk 3, and D15 on a stripe 3 of a hard disk 4. DP1 is obtained by performing an exclusive OR operation on D1 on a stripe 0 of a hard disk 2, D6 on a stripe 1 of a hard disk 3, D11 on a stripe 2 of a hard disk 4, and P3 on a stripe 3 of a first parity hard disk. DP2 is obtained by performing an exclusive OR operation on D2 on a stripe 0 of a hard disk 3, D7 on a stripe 1 of a hard disk 4, P2 on a stripe 2 of an odd even hard disk, and D12 on a stripe 3 of a hard disk 1. Therefore,  $DP_0 = D_0 \oplus D_5 \oplus D_{10} \oplus D_{15}$ ,  $DP_1 = D_1 \oplus D_6 \oplus D_{11} \oplus P_3$ , and so on.

## Working Principles of RAID 6 DP

- Double parity (DP): In addition to the horizontal XOR parity disk used in RAID 4, it adds another disk to store diagonal XOR parity data.
- P0 to P3 on the horizontal parity disk are the parity information of horizontal data on all data disks.
  - For example,  $P_0 = D_0 \text{ XOR } D_1 \text{ XOR } D_2 \text{ XOR } D_3$
- DP 0 to DP 3 in the diagonal parity disk represent the diagonal parity data for respective data disks and the horizontal parity disk.
  - For example,  $DP_0 = D_0 \text{ XOR } D_5 \text{ XOR } D_{10} \text{ XOR } D_{15}$



33      Huawei Confidential



- A RAID 6 array tolerates failures of up to two disks.
- Performance of a RAID 6 group: Dual-disk verification is used, and the performance is relatively slow. Therefore, RAID 6 applies to the following two scenarios:
  - Data is critical and should be consistently online and available.
  - The disk capacity is large (usually greater than 2 TB). The reconstruction of a large-capacity disk takes a long time. Data will be inaccessible for a long time if two disks fail at the same time. A RAID 6 array tolerates failure of another disk during the reconstruction of one disk. Some enterprises want to use a dual-redundancy RAID array for their large-capacity disks.

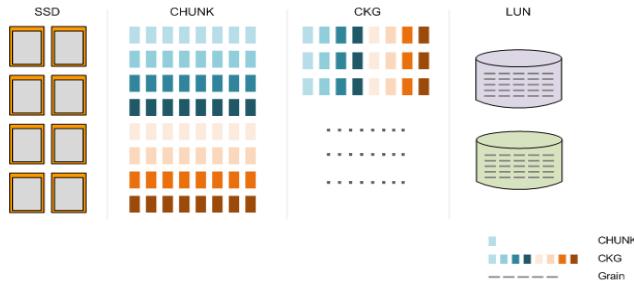
# Introduction to RAID 2.0

- **RAID 2.0**
  - RAID 2.0 is an enhanced RAID technology that effectively resolves the following problems: prolonged reconstruction of an HDD, and data loss if a disk is faulty during the long reconstruction of a traditional RAID group.
- **RAID 2.0+**
  - RAID 2.0+ provides smaller resource granularities (tens of KB) than RAID 2.0 to serve as the units of standard allocation and reclamation of storage resources, similar to VMs in computing virtualization. This technology is called virtual block technology.
- **Huawei RAID 2.0+**
  - Huawei RAID 2.0+ is a new RAID technology that overcomes traditional RAID issues. Huawei RAID 2.0+ evolves in line with the storage architecture virtualization to implement two-layer virtualized management instead of the traditional fixed management. Based on the underlying disk management that employs block virtualization (Virtual for Disk), RAID 2.0+ uses Smart-series efficiency improvement software to implement efficient resource management that features upper-layer virtualization (Virtual for Pool).

- Block virtualization is to divide disks into multiple contiguous storage spaces of a fixed size called a chunk (CK).

## RAID 2.0+ Block Virtualization

- If data is not evenly stored on SSDs, some heavily loaded SSDs may become the system bottleneck.
- The storage system uses RAID 2.0+ for fine-grained division of SSDs to evenly distribute data to all LUNs on each SSD and balance loads.



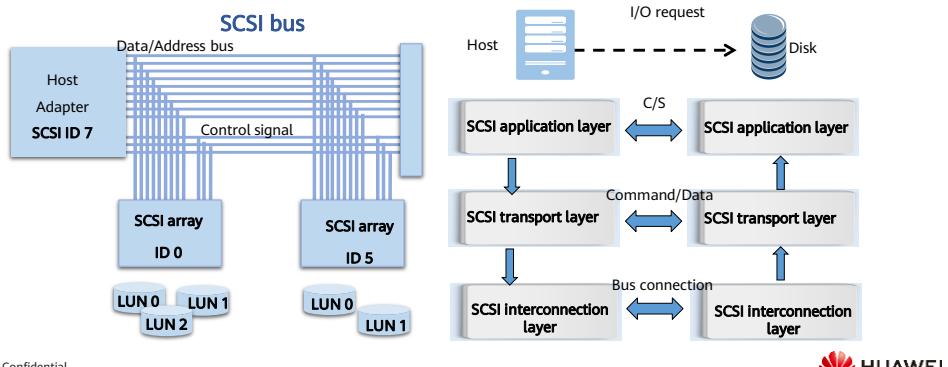
1. Multiple SSDs form a storage pool.
  2. Each SSD is then divided into CKs of a fixed size (typically 4 MB) for logical space management.
  3. CKs from different SSDs form chunk groups (CKGs) based on the RAID policy specified on DeviceManager.
  4. CKGs are further divided into grains (typically 8 KB). Grains are mapped to LUNs for refined management of storage resources.
- RAID 2.0+ has the following advantages over traditional RAID:
    - Balanced service loads for zero hotspots. Data is evenly distributed to all SSDs in a storage resource pool, ensuring no SSD becomes a hotspot, thereby lowering the SSD failure rate.
    - Quick reconstruction for a lowered data loss risk. Faulty SSDs trigger data reconstruction on all the other SSDs in the storage pool. This many-to-many reconstruction is rapid and significantly reduces data vulnerability.
    - All SSDs in a storage resource pool participate in reconstruction, and each SSD only needs to reconstruct a small amount of data. Therefore, the reconstruction process does not affect upper-layer applications.

# Contents

1. Storage Basics
2. Key Storage Technologies
  - RAID Technologies
  - Storage Protocol

## SCSI

- Small Computer System Interface (SCSI) is an interface technology developed for midrange computers and used for connecting between hosts and peripheral devices.



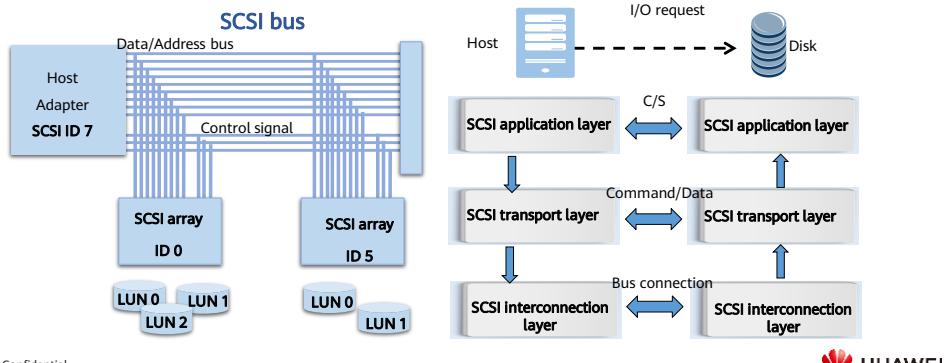
37      Huawei Confidential

HUAWEI

- Computers communicate with storage systems through buses. The bus is a path through which data is transferred from the source device to the target device. To put it simple, the high-speed cache of the controller functions as the source device and transfers data to target disks, which serve as the target devices. The controller sends a signal to the bus processor requesting to use the bus. After the request is accepted, the controller's high-speed cache sends data. During this process, the bus is occupied by the controller and other devices connected to the same bus cannot use it. However, the bus processor can interrupt the data transfer at any time and allow other devices to use the bus for operations of a higher priority.
- A computer has numerous buses, which are like high-speed channels used for transferring information and power from one place to another. For example, the universal serial bus (USB) port is used to connect an MP3 player or digital camera to a computer. The USB port is competent to the data transfer and charging of portable electronic devices that store pictures and music. However, the USB bus is incapable of supporting computers, servers, and many other devices.

## SCSI

- Small Computer System Interface (SCSI) is an interface technology developed for midrange computers and used for connecting between hosts and peripheral devices.

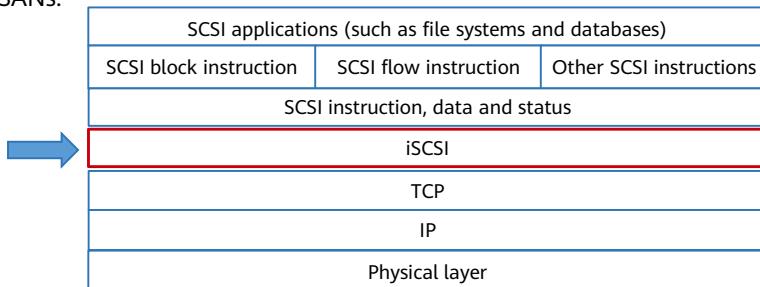


38      Huawei Confidential

- In this case, SCSI buses are applicable. SCSI, short for Small Computer System Interface, is an interface used to connect between hosts and peripheral devices including disk drives, tape drives, CD-ROM drives, and scanners. Data operations are implemented by SCSI controllers. Like a small CPU, the SCSI controller has its own command set and cache. The special SCSI bus architecture can dynamically allocate resources to tasks run by multiple devices in a computer. In this way, multiple tasks can be processed at the same time.

## iSCSI

- iSCSI encapsulates SCSI commands and block data into TCP packets and transmits the packets over an IP network. iSCSI uses mature IP network technologies to implement and extend SANs.

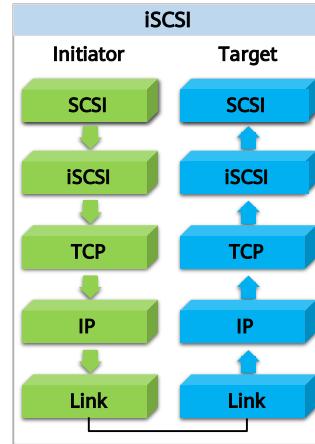


- The SCSI controller card is used to connect to multiple devices to form a network. The devices can communicate with each other on the network but cannot be shared on the Ethernet. If devices form a network through SCSI and the network can be mounted to an Ethernet, the devices can interconnect and share with other devices as network nodes. As a result, the iSCSI protocol evolved from SCSI. The IP SAN using iSCSI converts user requests into SCSI codes and encapsulates data into IP packets for transmission over the Ethernet.
- The iSCSI scheme was initiated by Cisco and IBM and then advocated by Adaptec, Cisco, HP, IBM, Quantum, and other companies. iSCSI offers a way of transferring data through TCP and saving data on SCSI devices. The iSCSI standard was drafted in 2001 and submitted to IETF in 2002 after numerous arguments and modifications. In Feb. 2003, the iSCSI standard was officially released. The iSCSI technology inherits advantages of traditional technologies and develops based on them. On one hand, SCSI technology is a storage standard widely applied by storage devices including disks and tapes. It has been keeping a fast development pace since 1986. On the other hand, TCP/IP is the most universal network protocol and IP network infrastructure is mature. The two points provide a solid foundation for iSCSI development.
- Prevalent IP networks allow data to be transferred over LANs, WANs, or the Internet using new IP storage protocols. The iSCSI protocol is developed by this philosophy. iSCSI adopts IP technical standards and converges SCSI and TCP/IP

protocols. Ethernet users can conveniently transfer and manage data with a small investment.

# iSCSI Initiator and Target

- Initiator
  - The SCSI layer generates command descriptor blocks (CDBs) and transfers them to the iSCSI layer.
  - The iSCSI layer generates iSCSI protocol data units (PDUs) and sends them to the target over an IP network.
- Target
  - The iSCSI layer receives PDUs and sends CDBs to the SCSI layer.
  - The SCSI layer interprets CDBs and gives responses when necessary.



- The iSCSI communication system inherits some of SCSI's features. The iSCSI communication involves an initiator that sends I/O requests and a target that responds to the I/O requests and executes I/O operations. After a connection is set up between the initiator and target, the target controls the entire process as the primary device.
- There are three types of iSCSI initiators: software-based initiator driver, hardware-based TCP offload engine (TOE) NIC, and iSCSI HBA. Their performance increases in that order.
- iSCSI targets include iSCSI disk arrays and iSCSI tape libraries.
- The iSCSI protocol defines a set of naming and addressing methods for iSCSI initiators and targets. All iSCSI nodes are identified by their iSCSI names. This method distinguishes iSCSI names from host names.
- iSCSI uses iSCSI names to identify initiators and targets. Addresses change with the relocation of initiator or target devices, but their names remain unchanged. When setting up a connection, an initiator sends a request. After the target receives the request, it checks whether the iSCSI name contained in the request is consistent with that bound with the target. If the iSCSI names are consistent, the connection is set up. Each iSCSI node has a unique iSCSI name. One iSCSI name can be used in the connections from one initiator to multiple targets. Multiple iSCSI names can be used in the connections from one target to multiple initiators.

## Discussion:

- We have learned the FC SAN and IP SAN. Now assume that two sites use different networks FC SAN and TCP/IP. How can storage devices at the two sites communicate with each other?
  - To converge Fibre Channel and TCP?



## Convergence of Fibre Channel and TCP

- Ethernet technologies and Fibre Channel technologies are both developing fast. Therefore, it is inevitable that IP SAN and FC SAN that are complementary coexist for a long time.
- Fibre Channel over a TCP/IP network:
  - iFCP
  - FCoE



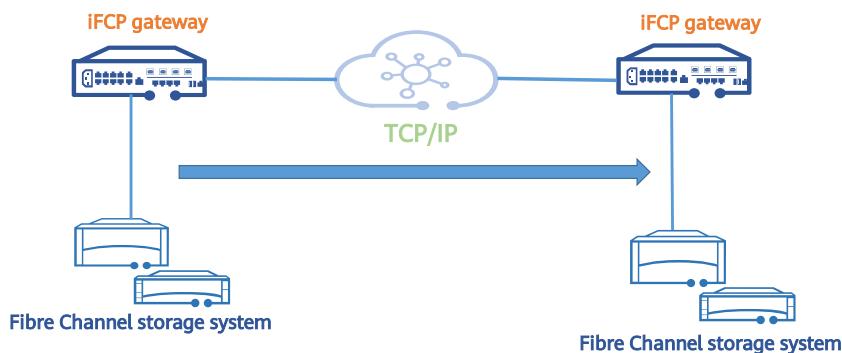
42      Huawei Confidential

 HUAWEI

- **Fibre Channel over IP (FCIP)** is an IETF proposed standard that defines the Fibre Channel architecture over TCP/IP links. FCIP uses the current IP protocol and facilities to connect the tunnels of two Fibre Channel SANs at different places.
- **Internet Fibre Channel Protocol (iFCP)** is a gateway-to-gateway protocol that provides Fibre Channel communication services for optical devices on TCP/IP networks. iFCP delivers congestion control, error detection, and recovery functions through TCP. The purpose of iFCP is to enable current Fibre Channel devices to interconnect and network at the line rate over an IP network. The frame address conversion method defined in this protocol allows Fibre Channel storage devices to be added to the IP-based network through transparent gateways.
- **Fibre Channel over Ethernet (FCoE)** transmits Fibre Channel signals over an Ethernet, so that Fibre Channel data can be transmitted at the backbone layer of a 10 Gbit/s Ethernet using the Fibre Channel protocol.
- **IP over Fiber Channel (IPFC)** uses the Fibre Channel connections between two servers as IP data exchange media. To do this, IPFC defines how to transmit IP packets over a Fibre Channel network. Like all other application protocols, IPFC is implemented by a device driver in an operating system. The **ifconfig** or **ipconfig** command is executed for local IP connections. Then the IPFC driver addresses the Fibre Channel HBA. After that, IP packets can be transmitted through Fibre Channel.

## iFCP

- Internet Fibre Channel Protocol (iFCP) is a gateway-to-gateway protocol that provides Fibre Channel communication services for optical devices on TCP/IP networks to implement end-to-end IP connection.



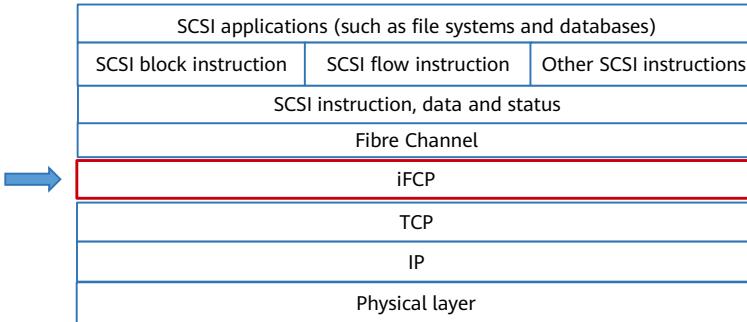
43      Huawei Confidential



- iFCP is a gateway-to-gateway protocol that provides Fibre Channel communication services for optical devices on TCP/IP networks to implement end-to-end IP connection. Fibre Channel storage devices, HBAs, and switches can directly connect to iFCP gateways. iFCP provides traffic control, error detection, and error recovery through TCP. It enables Fibre Channel devices to interconnect and network at the line rate over an IP network.
- The frame address conversion method defined in the iFCP protocol allows Fibre Channel storage devices to be added to the TCP/IP-based network through transparent gateways. iFCP can replace Fibre Channel to connect to and group Fibre Channel devices using iFCP devices. However, iFCP does not support the merge of independent SANs, and therefore a logical SAN cannot be formed. iFCP outstands in supporting SAN interconnection as well as gateway zoning, allowing fault isolation and breaking the limitations of point-to-point tunnels. In addition, iFCP enables end-to-end connection between Fibre Channel devices. As a result, the interruption of TCP connection affects only a communication pair. SANs that adopt iFCP support fault isolation and security management, and deliver higher reliability than SANs that adopt FCIP.

## iFCP Protocol Stack

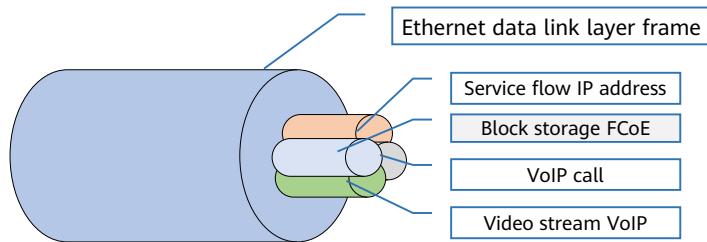
- iFCP is between Fibre Channel and TCP/IP, which means that iFCP can interwork with either Fibre Channel or TCP/IP.



- The main function of the iFCP protocol layer is to transport Fibre Channel frame images between locally and remotely attached N\_Ports. When transporting frames to a remote N\_Port, the iFCP layer encapsulates and routes the Fibre Channel frame comprising each Fibre Channel information unit, and transmits the frame via a predetermined TCP connection over the IP network.
- In the IP SAN that uses iFCP, iFCP devices take the place of Fibre Channel switches, which means that iFCP switches can also function as Internet Storage Name Servers (iSNSs) to provide the name discovery service for terminal nodes. The iFCP switch allocates a 4-byte IP address to each Fibre Channel terminal node. When a Fibre Channel device sends an SNS name query request, the request is intercepted by the iFCP switch and interpreted by the iSNS server.

## FCoE

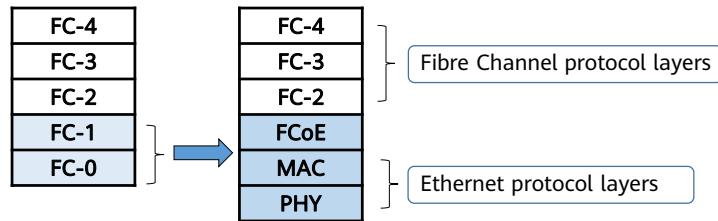
- Fibre Channel over Ethernet (FCoE) allows the transmission of LAN and FC SAN data on the same Ethernet link. This reduces the number of devices, cables, and network nodes in a data center, as well as power consumption and cooling loads, simplifying management.
- FCoE encapsulates FC data frames into Ethernet frames and allows service traffic on a LAN and SAN to be transmitted over the same Ethernet.



- FCoE offers standard Fibre Channel services, including discovery, global naming, and zoning. These services run in the same way as the original Fibre Channel services with low latency and high performance.
- From the perspective of Fibre Channel, FCoE enables Fibre Channel to be carried by the Ethernet Layer 2 link. From the perspective of the Ethernet, FCoE is an upper-layer protocol that the Ethernet carries, like IP or IPX.

## FCoE Protocol Encapsulation

- FCoE encapsulates contents in the FC-2 and above layers into Ethernet packets for transmission.



- The Fibre Channel protocol stack has five layers. FC-0 defines the medium type, FC-1 defines the frame coding and decoding mode, FC-2 defines the frame division protocol and flow control mechanism, FC-3 defines general services, and FC-4 defines the mapping from upper-layer protocols to Fibre Channel.

## Discussion:

- What are the application scenarios of FCoE?
- What are the application scenarios of iFCP?



## Quiz

1. Which of the following statements about FC SAN are true?
  - A. Fibre Channel switches are required.
  - B. Ethernet switches are required.
  - C. Fibre Channel links cannot be used between storage devices.
  - D. Data packets comply with the Fibre Channel protocol stack.
2. The performance of SATA disks is better than that of SAS disks.
  - A. True
  - B. False

- Answers:
  - AD
  - B

# Summary

In this course, we covered:

- Mainstream data storage modes and network topologies
- RAID and Huawei RAID 2.0+ block virtualization technologies
- Differences and relationships between centralized storage and distributed storage
- Storage protocols and their application scenarios

In the next course, we will learn the network technologies.

## Recommendations

- Huawei iLearning
  - <https://e.huawei.com/en/talent/#/>
- Huawei Support Case Library
  - <https://support.huawei.com/enterprise/en/knowledge?lang=en>

## Acronyms and Abbreviations

FC: Fibre Channel

FCIP: Fibre Channel over IP

FCoE: Fibre Channel over Ethernet

iFCP: Internet Fibre Channel Protocol

iSCSI: Internet Small Computer System Interface

IPFC: IP over Fiber Channel

## Acronyms and Abbreviations

IOPS: Input/Output per second

MTBF: Mean Time Between Failure

NAS: Network Attached Storage

RAID: Redundant Array of Independent Disks

SAN: Storage Area Network

SCSI: Small Computer System 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.

Copyright©2021 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



# Network Technology Basics



# Foreword

- Network technologies are the basis for the interconnection of all platforms and services. What exactly is a network? What are the basic principles of network communication? And what are the common network technologies? This course will answer these questions and more.

# Objectives

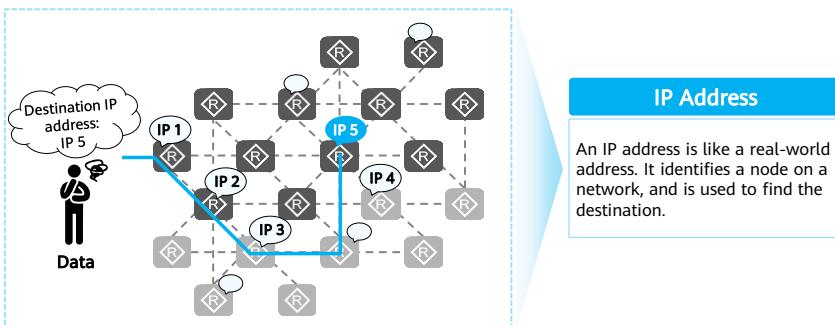
- Upon completion of this course, you will be able to:
  - Understand the classification and subnetting of IP addresses.
  - Understand the basic principles of network communication.
  - Be familiar with the operating principles of switches and routers.
  - Understand the technical principles and basic configuration methods of VLAN.

# Contents

- 1. IP Address Basics**
2. Introduction to Network Technologies
3. Switching Basics
4. Routing Basics

## What Is an IP Address?

- An IP address is a unique logical address used to identify a device that sends or receives data packets on a network.
- The functions of an IP address are to:
  - Identify a host or network device (identifying its network interface and indicating its location on the network).
  - Implement network addressing



5    Huawei Confidential

 HUAWEI

- On an IP network, to connect a PC to the Internet, you need to apply an IP address for the PC. An IP address is like a real-world address. It identifies a node on a network, and is used to find the destination. Global network communication is based on IP addresses.
- An IP address is an attribute of an interface on a network device, not an attribute of the network device itself. To assign an IP address to a device is to assign an IP address to an interface of the device actually. If a device has multiple interfaces, each interface requires at least one IP address.
- Note: An interface that requires an IP address is usually the interface on a router or a computer.

## IP Address Format

- An IPv4 address has 32 bits.
- An IPv4 address is usually represented in dotted decimal notation.

Dotted decimal notation	Decimal digit	192	168	10	1	4 bytes				
Binary digit	11000000	10101000	00001010	00000001	32 bits					
Decimal-to-binary conversion	Power	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	
	Bit	1	1	0	0	0	0	0	0	
$= 128 + 64 = 192$										

- IPv4 address range: 0.0.0.0–255.255.255.255

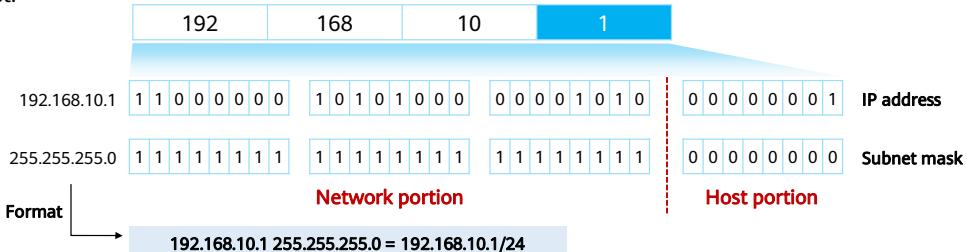
- IP address format:
  - An IP address has 32 bits and consists of four bytes. For the convenience of reading and writing, an IP address is usually in the format of dotted decimal notation.
- Dotted decimal notation:
  - This type of IP address format is commonly used because it is easy to understand. However, a communication device uses binary digits to calculate the IP address. Therefore, it is necessary to master the conversion between decimal and binary digits.
- IPv4 address range:
  - 00000000.00000000.00000000.00000000–11111111.11111111.11111111.11111111 in binary, and 0.0.0.0–255.255.255.255 in decimal.

# IP Address Structure

- **Network portion:** identifies a network segment.
- **Host portion:** uniquely identifies a host on a network segment.



- **Subnet mask:** specifies which portion of an address refers to the subnet and which portion refers to the host.



- An IPv4 address consists of two parts:
  - Network portion: identifies a network segment.
    - IP addresses do not show any geographical information. The network bits indicate the segment to which an IP address belongs.
    - Network devices with same network bits are located on the same network, regardless of their physical locations.
  - Host portion: uniquely identifies a host on a network segment.
- A subnet mask is also called a netmask:
  - Same as an IP address, a subnet mask consists of 32 bits, and is also displayed in dotted decimal notation generally.
  - A subnet mask is not an IP address. A subnet mask written in the binary format consists of consecutive 1s and 0s.
  - Generally, the number of 1s in a subnet mask is the length of the subnet mask. For example, the length of the subnet mask 0.0.0.0 is 0, and that of 252.0.0.0 is 6.

- How to identify the network and host bits in an IP address: In a subnet mask, bits with the value of 1 correspond to the network bits in an IP address, while bits with the value of 0 correspond to the host bits. In other words, the number of 1s in a subnet mask equals to the number of network bits in an IP address, while the number of 0s equals to the number of host bits.

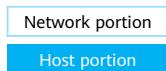
## IP Address Classes (Classified Addressing)

- IP addresses are classified into five classes to facilitate IP address management and networking.

Class A	0NNNNNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	0.0.0.0–127.255.255.255	Assigned to hosts
Class B	10NNNNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	128.0.0.0–191.255.255.255	
Class C	110NNNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	192.0.0.0–223.255.255.255	
Class D	1110NNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	224.0.0.0–239.255.255.255	
Class E	1111NNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	240.0.0.0–255.255.255.255	

- Default subnet masks:

- Class A: 8 bits, 0.0.0.0–127.255.255.255/8
- Class B: 16 bits, 128.0.0.0–191.255.255.255/16
- Class C: 24 bits, 192.0.0.0–223.255.255.255/24



- IP addresses are classified into five classes to facilitate IP address management and networking:
  - The easiest way to determine the class of an IP address is to check the first bits in its network bits. The class fields of class A, class B, class C, class D, and class E are binary numbers 0, 10, 110, 1110, and 1111, respectively.
  - Class A, B, and C addresses are unicast IP addresses (except some special addresses). Only these three types of addresses can be assigned to hosts.
  - Class D addresses are multicast IP addresses.
  - Class E addresses are used for special experimental purposes.
  - This section focuses only on class A, B, and C addresses.
- Comparison between class A, B, and C addresses:
  - Networks using class A addresses are called class A networks. Networks using class B addresses are called class B networks. Networks using class C addresses are called class C networks.
  - The number of network bits of a class A network is 8. The number of network bits is small, so the number of addresses that can be assigned to the hosts is large. The first bit in the network bits of a class A network is always 0. The address range is 0.0.0.0–127.255.255.255.
  - The number of network bits of a class B network is 16, and the first two bits are always 10. The address range is 128.0.0.0–191.255.255.255.

- The number of network bits of a class C network is 24. The number of network bits is large, so the number of addresses that can be assigned to the hosts is small. The first three bits in the network bits of a class C network are always 110. The address range is 192.0.0.0-223.255.255.255.
- Note:
  - A host refers to a router or a computer, and the IP address of an interface on a host refers to the host IP address.
  - Multicast address: Multicast refers to one-to-many message transmission.

# Public and Private IP Addresses

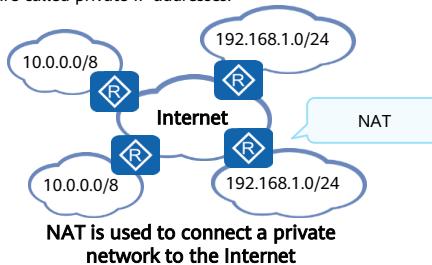
- **Public IP address**

- Public IP addresses are assigned by the Internet Corporation for Assigned Names and Numbers (ICANN) to ensure that each IP address is unique on the Internet. Public IP addresses can be used for accessing the Internet.

- **Private IP address**

- Some networks do not need to connect to the Internet, for example, a network in a closed lab of a university. However, the IP addresses of network devices in the lab network still need to be unique to avoid conflicts. Some IP addresses of classes A, B, and C are reserved for this kind of situation. These IP addresses are called private IP addresses.

- Class A: 10.0.0.0–10.255.255.255
    - Class B: 172.16.0.0–172.31.255.255
    - Class C: 192.168.0.0–192.168.255.255



NAT is used to connect a private network to the Internet



- Private IP addresses are used to resolve IP address shortage. They are used for internal networks or hosts, and cannot be used for public networks.
  - Public IP address: Network devices connected to the Internet must have public IP addresses assigned by ICANN.
  - Private IP address: increases the number of available IP addresses. A private IP address can be repeatedly used on different private networks.
- Connecting a private network to the Internet: A private network is not allowed to directly connect to the Internet because it uses a private IP address. Due to actual requirements, many private networks also want to be connected to the Internet to communicate with the Internet or other private networks through the Internet. The interconnection between a private network and the Internet is implemented through the network address translation (NAT) technology.
- Note:
  - NAT is used to translate private IP addresses into public IP addresses.

- ICANN is a standards organization that oversees global IP address allocation.

## Special IP Addresses

- There are some special IP addresses that have special meanings and functions.

Special IP Address	IP Address Range	Function
Limited broadcast address	255.255.255.255	Packets that use this address as the destination address will be sent to all hosts on the same network segment. (The destination range is limited by the gateway.)
Any address	0.0.0.0	This address is the network address of any network, or the IP address of an interface on a network.
Loopback address	127.0.0.0/8	This address is used to test the software system of a device.
Link-local address	169.254.0.0/24	When a host fails to obtain an IP address automatically, the host can use a link-local address for temporary communication.

- 255.255.255.255
  - This address is called a limited broadcast address and can be used as the destination IP address of an IP packet.
  - After receiving an IP packet whose destination IP address is a limited broadcast address, a router stops forwarding the IP packet.
- 0.0.0.0
  - If this address is used as a network address, it refers to the network address of any network. If this address is used as a host address, it refers to an interface IP address of a host on the network.
  - For example, when a host does not obtain an IP address during startup, it can send a DHCP Request packet with the source IP address being 0.0.0.0 and the destination IP address being a limited broadcast address to the network. The DHCP server will assign an available IP address to the host after receiving the DHCP Request packet.
- 127.0.0.0/8
  - This address is a loopback address that can be used as the destination IP address of an IP packet. It is used to test the software system of the device.
  - An IP packets whose destination IP address is a loopback address cannot leave the device which sends the packet.

- 169.254.0.0/16
  - If a network device is configured to automatically obtain an IP address but does not find an available DHCP server on the network, the device uses an IP address on the 169.254.0.0/16 network segment for temporary communication.
- Note: DHCP is used to dynamically allocate network configuration parameters, such as IP addresses.

## Subnet Mask and Available Host Address

- Generally, the network range defined by a network ID is called a network segment.
- Subnet mask:** Used to calculate the network ID (network address) and host ID (host address) in an IP address.

Example: 192.168.10.0/24

192	168	10	00000000
-----	-----	----	----------

- Broadcast address:** Used as a special destination address to send data to all hosts on the network.

Example: 192.168.10.255/24

192	168	10	11111111
-----	-----	----	----------

- Available address:** Assigned to a node or an interface of a device on a network.

Example: 192.168.10.1/24

192	168	10	00000001
-----	-----	----	----------

### Note

- Network addresses and broadcast addresses cannot be used as the address of nodes or network devices.
- The number of available IP addresses on a network segment is  $2^n - 2$  ( $n$  is the number of host bits).

- Broadcast address
  - Each bit of the host ID is 1.
  - It cannot be allocated to a specific interface on a host.
- Available address
  - It is also called a host address and can be allocated to a specific interface on a host.
- Calculation of the number of available IP addresses on a network segment
  - If the number of host bits of a network segment is  $n$ , the number of IP addresses on the network segment is  $2^n$ , and the number of available host addresses is  $2^n - 2$  (subtracting the network address and broadcast address).

## IP Address Calculation

- Calculate the network address, broadcast address, and number of available addresses of the class B address 172.16.10.1/16.

	172	16	00001010	00000001	
IP address	1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 0	0 0 0 0 1 0 1 0	0 0 0 0 0 0 0 1	
Subnet mask	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	Change all host bits to 0, and the network address is obtained. 172.16.0.0
Network address	1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	Change all host bits to 1, and the broadcast address is obtained. 172.16.255.255
Broadcast address	1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 0	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	
Number of IP addresses	$2^{16}=65536$				
Number of available IP addresses	$2^{16}-2=65534$				
Range of available IP addresses	172.16.0.1-172.16.255.254				

12 Huawei Confidential



### Extra Practice

Calculate the network address, broadcast address, and number of available addresses of the class A address 10.128.20.10/8.

- Network address: Change all host bits of an IP address to 0, and the result is the network address of the network to which the IP address belongs.
- Broadcast address: Change all host bits of an IP address to 1, and the result is the broadcast address of the network to which the IP address belongs.
- Number of IP addresses:  $2^n$ , where  $n$  indicates the number of host bits.
- Number of available IP addresses:  $2^n - 2$ , where  $n$  indicates the number of host bits.
- Answer to the practice:
  - Network address: 10.0.0.0
  - Broadcast address: 10.255.255.255
  - Number of IP addresses: 224
  - Number of available IP addresses: 222 (224 - 2)
  - Range of available IP addresses: 10.0.0.1-10.255.255.254

# Subnetting

- Why do we need subnetting?
- The variable length subnet mask (VLSM) technology is used in subnetting.
  - VLSM allows an organization to divide a network into multiple subnets based on the network scale for different departments to use.
- For example, a company is assigned a class C IP address 201.222.5.0. Assume that 20 subnets are required and each subnet contains five hosts. How should we divide the subnets?

Subnet Address	Available Host Addresses
201.222.5.8/29	201.222.5.9-201.222.5.14
201.222.5.16/29	201.222.5.17-201.222.5.22
...	...
201.222.5.232/29	201.222.5.233-201.222.5.238
201.222.5.240/29	201.222.5.241-201.222.5.246

- Why do we need subnetting?
- In practice, if a class A network is assigned to an organization but the number of hosts in the organization is less than 16777214, a large number of IP addresses will be idle and wasted. Therefore, a more flexible method is required to divide the network based on the network scale. The idea is to divide a network into multiple subnets for different organizations to use through VLSM. VLSM can be used on both public networks and enterprise networks.
- In the preceding example, 201.222.5.0 is a class C address, whose default subnet mask is 24. Assume that 20 subnets are required and each subnet contains five hosts. The last byte (8 bits) of 201.222.5.0 should be divided into subnet bits and host bits.
- The number of subnet bits determines the number of subnets. As this address is a class C address, the total number for subnet bits and host bits is 8. Because the value 20 is in the range of  $2^4$  (16) to  $2^5$  (32), 5 bits should be reserved for subnet bits. The 5-bit subnet part allows a maximum of 32 subnets. The 3 bits left are host bits, which means that there are a maximum of  $2^3$  (8) IP addresses. Except for one network address and one broadcast address, six addresses can be used by hosts.
- The network segments are:
  - 201.222.5.0-201.222.5.7

- 201.222.5.8-201.222.5.15
- 201.222.5.16-201.222.5.23
- ...
- 201.222.5.232-201.222.5.239
- 201.222.5.240-201.222.5.247
- 201.222.5.248-201.222.5.255

# Contents

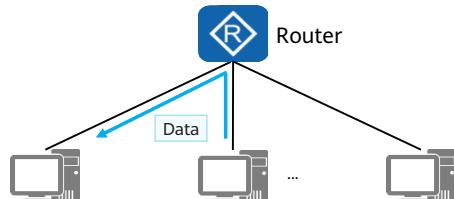
1. IP Address Basics
2. **Introduction to Network Technologies**
  - Network Basics
    - Common Network Devices
    - Introduction to Common Protocols
3. Switching Basics
4. Routing Basics

# Concept of Network Communication

- Communication refers to the information transfer and exchange between people, between people and things, and between things through a certain medium and action.
- Network communication refers to communication between terminal devices through a computer network.
- Examples of network communication:



A. Files are transferred between two computers (terminals) through a network cable.



B. Files are transferred among multiple computers (terminals) through a router.

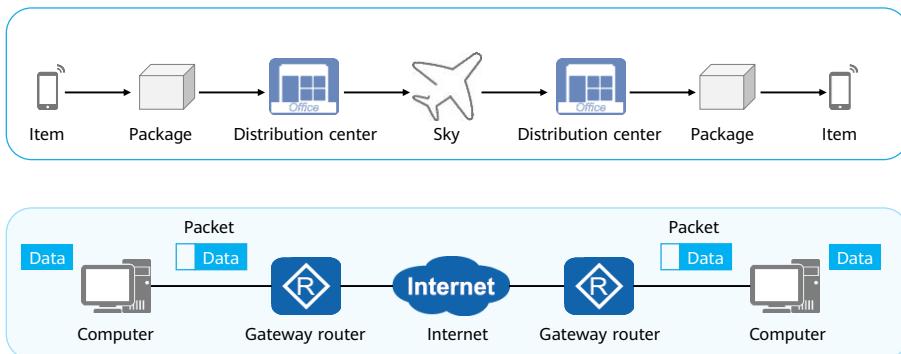


C. A computer (terminal) downloads files through the Internet.

- Examples of network communication:
  - A: Two computers are connected through a network cable to form a simple network.
  - B: A router (or switch) and multiple computers form a small-scale network. In such a network, files can be freely transferred between every two computers through a router.
  - C. If a computer wants to download files from a website, it must access the Internet first.
- The Internet is the largest computer network in the world. Its predecessor, Advanced Research Projects Agency Network (ARPANET), was born in 1969. The wide popularization and application of Internet is one of the signs of entering the information age.

## Information Transfer Process

- Virtual information transfer is similar to real object transfer.



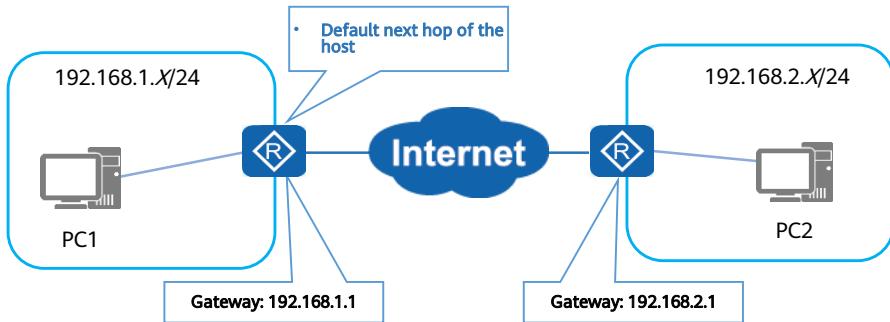
- Comparison between the express delivery process and network communication process:
- Items to be delivered:
  - The information (or data) generated by the application
- The item is packed into a package and pasted with a package label containing the receiver's name and address.
  - The application packs the data into an original data payload and adds a header and a tail to form a packet. The important information in the packet is the address of the receiver, that is, the destination address.
  - Encapsulation is a process in which new information segments are added to an information unit, forming a new information unit.
- The package is delivered to a distribution center in which packages are sorted based on the destination addresses. The packages destined for the same city are placed in the same plane for airlift.
  - The packet reaches the gateway through a network cable. After receiving the packet, the gateway decapsulates the packet, obtains the destination address, re-encapsulates the packet, and sends the packet to different

routers based on the destination address. The packet is transmitted through the gateway and router, leaves the local network, and is transmitted through the Internet.

- The network cable is the medium for information transmission, and plays the same role as the highway for item transmission.

- After the plane arrives at the destination airport, the packages are taken out for sorting, and the packages destined for the same area are sent to the same distribution center.
  - The packet is transmitted through the Internet and reaches the local network where the destination address resides. The gateway or router of the local network decapsulates and encapsulates the packet, and then determines the next-hop router according to the destination address. Finally, the packet reaches the gateway of the network where the destination computer resides.
- The distribution center sorts the packages according to the destination addresses on the packages. The courier delivers the packages to the receiver. The receiver unpacks the package, confirms that the items are intact, and signs for the package. The entire express delivery process is complete.
  - After the packet reaches the gateway of the network where the destination computer resides, the gateway decapsulates and encapsulates the packet, and then sends the packet to the corresponding computer according to the destination address. After receiving the packet, the computer verifies the packet. If the packet passes verification, the computer accepts the packet and sends the data payload to the corresponding application program for processing. A complete network communication process is complete.

## What Is a Gateway?

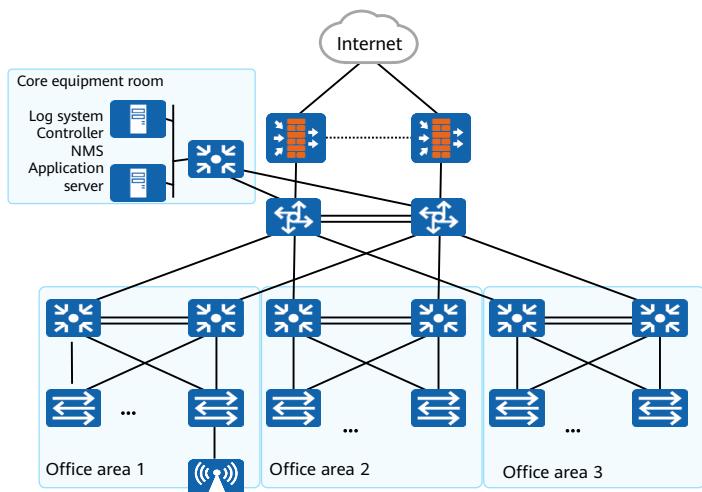


- A gateway is also called an inter-network connector or a protocol converter. By default, a gateway implements network interconnection above the network layer.
- Just like you must walk through a door when entering a room, information sent from one network or network segment to another must pass through a gateway. We can say the gateway is the door to another network.
- Functions of a gateway — A gateway plays significant roles in not only its role but also its configuration:
  - When a host (such as a PC, server, router, or firewall) wants to access another network segment, the gateway is responsible for sending ARP packets, and receiving and forwarding subsequent data packets.
  - After the gateway is configured, the default route is generated on the host, with the next hop being the gateway.

# Basic Architecture of a Communication Network

- Communication network

A communication network consists of routers, switches, firewalls, PCs, network printers, servers, and more.



- Function

The basic function of a communication network is to implement data communication.

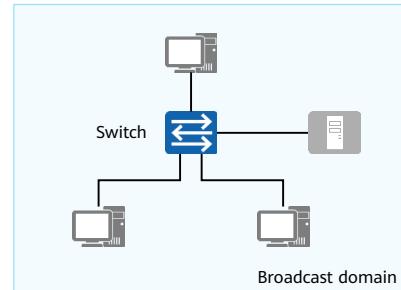
19    Huawei Confidential

HUAWEI

- Take the enterprise data center network (DCN) as an example. The major requirements of an enterprise for the DCN include service operation and computing, data storage, and service access.
- The DCN thereby needs to enable device-device and device-user interconnection and provide external access capabilities for services. Devices on such a network collaborate with each other to implement communication:
  - Access switches connect to user hosts in office areas.
  - Aggregation switches aggregate traffic from access switches.
  - Routers forward traffic between different office areas and between internal and external networks.
  - Firewalls implement access control for areas of different security levels and between internal and external networks to ensure secure access.

## Network Device - Switch

- As the device closest to end users, a switch connects end users to a network and forwards data frames. A switch can:
  - Connect terminals (such as PCs and servers) to the network.
  - Isolate collision domains.
  - Broadcast unknown packets.
  - Learn MAC addresses and maintain the MAC address table.
  - Forward packets based on the MAC address table.



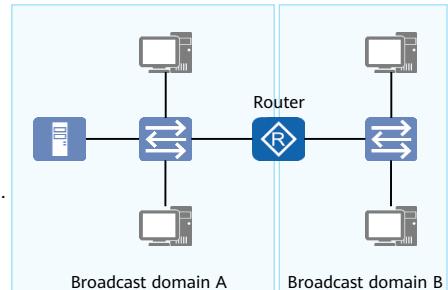
- Switch:

- Generally, on a campus network, switches are closest to end users, and Layer 2 switches (also known as Ethernet switches) are deployed at the access layer. Layer 2 refers to the data link layer of the TCP/IP model.
- An Ethernet switch can implement the following functions: data frame switching, access of end users, basic access security, and Layer 2 link redundancy.
- Broadcast domain: a group of nodes, among which a broadcast packet from one node can reach all the other nodes.
- Collision domain: an area where a collision occurs when two devices on the same network send packets at the same time.
- Media Access Control (MAC) address: uniquely identifies a network interface card (NIC) on a network. Each NIC requires and has a unique MAC address.

- MAC address table: exists on each switch and stores the mappings between MAC addresses and switch interfaces.

## Network Device - Router

- Working at the network layer, a router forwards data packets on the Internet. Based on the destination address in a received packet, a router selects a path to send the packet to the next router or destination. The last router on the path is responsible for sending the packet to the destination host. A router can:
  - Implement communication between networks of the same type or different types.
  - Isolate broadcast domains.
  - Maintain the routing table and run routing protocols.
  - Select routes and forward IP packets.
  - Implement WAN access and network address translation (NAT).
  - Connect Layer 2 networks built through switches.



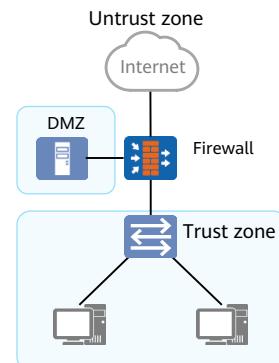
## Discussion

- What are the differences between a Layer 2 switch and a router that are both used for network connection?
- What are their application scenarios?



## Network Device - Firewall

- As a network security device, a firewall is used to ensure secure communication between two networks. It monitors, restricts, and modifies data flows passing through it to shield the information, structure, and running status of internal networks from the public network. A firewall can:
  - Isolate networks of different security levels.
  - Implement access control (using security policies) between networks of different security levels.
  - Perform user identity authentication.
  - Implement remote access.
  - Encrypt data and provide virtual private network (VPN) services.
  - Implement NAT.
  - Provide other security functions.



23 Huawei Confidential



- Firewall:

- Located between two networks of different trust levels (for example, an enterprise intranet and the Internet), a firewall controls the communication between the two networks and forcibly implements unified security policies to prevent unauthorized access to key information resources, ensuring system security.

# Contents

1. IP Address Basics
2. **Introduction to Network Technologies**
  - Network Basics
  - **Network Reference Model and Data Encapsulation**
  - Introduction to Common Protocols
3. Switching Basics
4. Routing Basics

## OSI Reference Model

- To achieve compatibility between networks and help vendors produce compatible network devices, the International Organization for Standardization (ISO) launched the Open Systems Interconnection (OSI) reference model in 1984. It was quickly adopted as the basic model for computer network communication.

7. Application layer	Provides interfaces for applications.
6. Presentation layer	Converts data formats to ensure the application layer of one system can identify and understand the data generated by the application layer of another system.
5. Session layer	Establishes, manages, and terminates sessions between two parties.
4. Transport layer	Establishes, maintains, and cancels one-time end-to-end data transmission processes, controls transmission speeds, and adjusts data sequencing.
3. Network layer	Defines logical addresses and transfers data from sources to destinations.
2. Data link layer	Encapsulates packets into frames, transmits frames in P2P or P2MP mode, and implements error checking.
1. Physical layer	Transmits bit streams over transmission media and defines electrical and physical specifications.

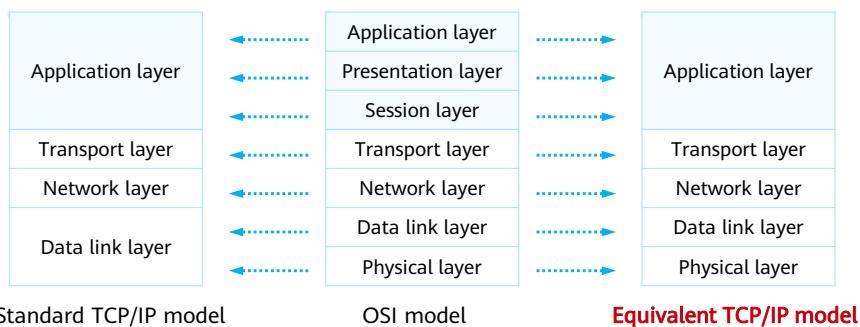
- The Open Systems Interconnection (OSI) model was included in the ISO 7489 standard and released in 1984. ISO stands for International Organization for Standardization.
- The OSI reference model is also called the seven-layer model. The seven layers from bottom to top are as follows:
  - Physical layer: transmits bit streams between devices and defines physical specifications such as electrical levels, speeds, and cable pins.
  - Data link layer: encapsulates bits into octets and octets into frames, uses link layer addresses (MAC addresses in Ethernet) to access media, and implements error checking.
  - Network layer: defines logical addresses for routers to determine paths and transmits data from source networks to destination networks.
  - Transport layer: implements connection-oriented and non-connection-oriented data transmission, as well as error checking before retransmission.
  - Session layer: establishes, manages, and terminates sessions between entities at the presentation layer. Communication at this layer is implemented through service requests and responses transmitted between

applications on different devices.

- Presentation layer: provides data encoding and conversion functions so that data sent by the application layer of one system can be identified by the application layer of another system.
- Application layer: provides network services for applications and is closest to users.

## TCP/IP Reference Model

- The TCP/IP reference model has become the mainstream reference model of the Internet because the TCP and IP protocols are widely used and the OSI model is too complex.



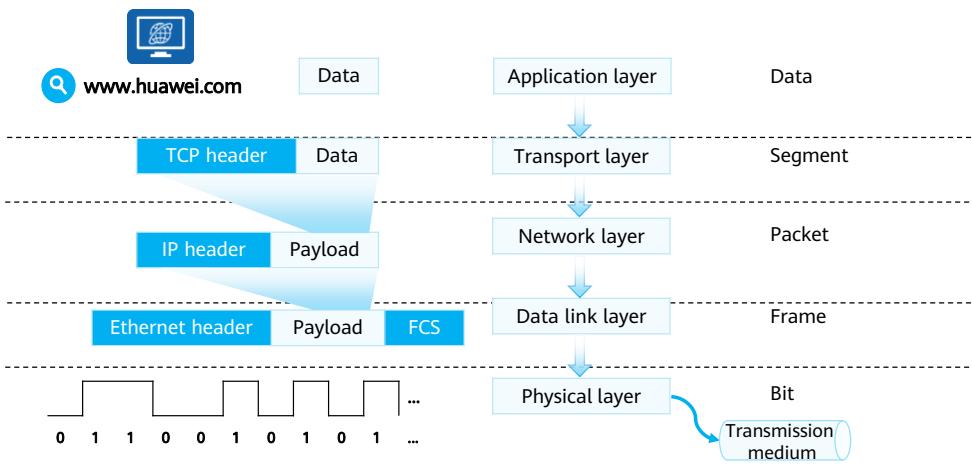
- Similar to the OSI model, the Transmission Control Protocol/Internet Protocol (TCP/IP) model adopts a hierarchical architecture, and adjacent layers are closely related.
- The standard TCP/IP model combines the data link layer and physical layer in the OSI model into the network access layer. This division mode is contrary to the actual protocol formulation. Therefore, the equivalent TCP/IP model that integrates the standard TCP/IP model and the OSI model is proposed. Contents in the following slides are based on the equivalent TCP/IP model.
- TCP/IP was originated from a packet switched network research project funded by the US government in the late 1960s. Since the 1990s, the TCP/IP model has become the most commonly used networking model for computer networks. It is a truly open system, because the definition of the protocol suite and its multiple implementations can be easily obtained at little or even no cost. It thereby became the basis of the Internet.
- Like the OSI reference model, the TCP/IP model is developed in different layers, each of which is responsible for different communication functions. The difference is, the TCP/IP model has a simplified hierarchical structure that consists of only five layers: application layer, transport layer, network layer, data

link layer, and physical layer. As shown in the figure, the TCP/IP protocol stack corresponds to the OSI reference model and covers all layers in the OSI reference model. The application layer contains all upper-layer protocols in the OSI reference model.

- The TCP/IP protocol stack supports all standard physical-layer and data-link-layer protocols. The protocols and standards at the two layers will be further discussed in following chapters.

- Comparison between the OSI reference model and TCP/IP protocol stack:
  - Similarities
    - They are both hierarchical and both require close collaboration between layers.
    - They both have the application layer, transport layer, network layer, data link layer, and physical layer. (Note: The TCP/IP protocol stack is divided into five layers here to facilitate comparison. In many documents, the data link layer and physical layer of TCP/IP are combined into the data link layer, which is also called network access layer.)
    - They both use the packet switching technology.
    - Network engineers must understand both models.
  - Differences
    - TCP/IP includes the presentation layer and session layer into the application layer.
    - TCP/IP has a simpler structure with fewer layers.
    - TCP/IP standards are established based on practices during the Internet development and are thereby highly trusted. In comparison, the OSI reference model is based on theory and serves as a guide.

## Data Encapsulation on the Sender



28 Huawei Confidential



- Assume that you are using a web browser to access Huawei's official website. After you enter the website address and press **Enter**, the following events occur on your computer:
  - Internet Explorer (application) invokes HTTP (application-layer protocol) to encapsulate the application-layer data. (**Data** in the figure should also include the HTTP header, which is not shown here.)
  - HTTP uses TCP to ensure reliable data transmission and thereby transmits the encapsulated data to the TCP module.
  - The TCP module adds the corresponding TCP header information (such as the source and destination port numbers) to the data transmitted from the application layer. The protocol data unit (PDU) is called a segment.
  - On an IPv4 network, the TCP module sends the encapsulated segment to the IPv4 module at the network layer. (On an IPv6 network, the segment is sent to the IPv6 module for processing.)
  - After receiving the segment from the TCP module, the IPv4 module encapsulates the IPv4 header. Here, the PDU is called a packet.
  - Ethernet is used as the data link layer protocol. Therefore, after the IPv4 module completes encapsulation, it sends the packet to the Ethernet module (such as the Ethernet adapter) at the data link layer for processing.
  - After receiving the packet from the IPv4 module, the Ethernet module adds

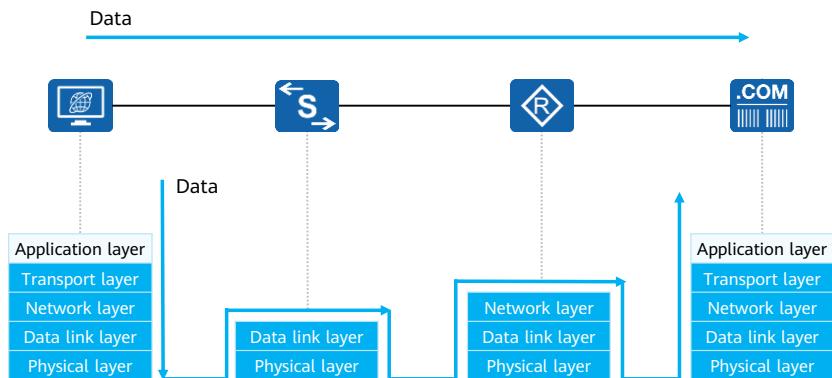
the corresponding Ethernet header and FCS frame trailer to the packet.

Now, the PDU is called a frame.

- After the Ethernet module completes encapsulation, it sends the data to the physical layer.
- Based on the physical media, the physical layer converts digital signals into electrical signals, optical signals, or electromagnetic (wireless) signals.
- The converted signals are then transmitted on the network.

## Data Transmission on the Intermediate Network

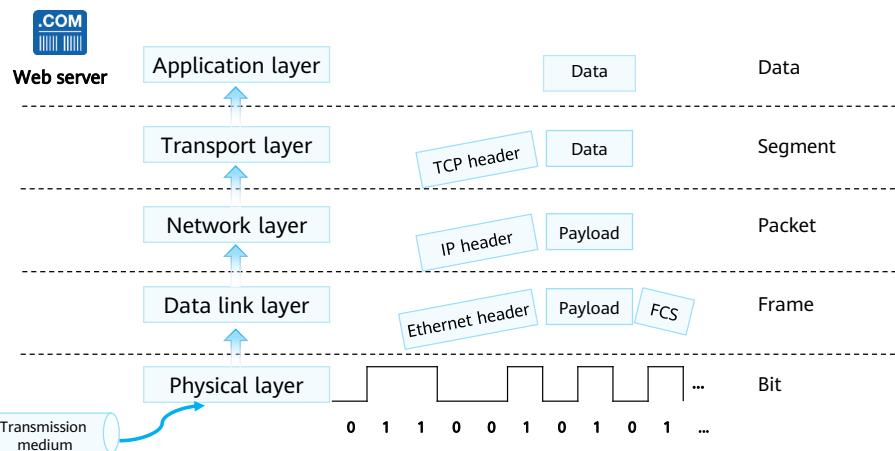
- Encapsulated data is transmitted on the network.



- In most cases:

- A Layer 2 device (such as an Ethernet switch) only decapsulates the Layer 2 header of the data and performs the corresponding switching operation based on the Layer 2 header information.
- A Layer 3 device (such as a router) only decapsulates the Layer 3 header and performs the corresponding routing operation based on the Layer 3 header information.
- Note: The details and principles of switching and routing will be described in the following chapters.

## Data Decapsulation on the Receiver



- After being transmitted over the intermediate network, the data finally reaches the destination server. Based on the information in different protocol headers, the data is decapsulated layer by layer, processed, transmitted, and finally sent to the application on the web server for processing.

# Contents

1. IP Address Basics
2. **Introduction to Network Technologies**
  - Network Basics
  - Network Reference Model and Data Encapsulation
  - Introduction to Common Protocols
3. Switching Basics
4. Routing Basics

## Common TCP/IP Protocols

- The TCP/IP protocol stack defines a set of standard protocols.

Application layer	Telnet HTTP	FTP SMTP	TFTP DNS	SNMP DHCP
Transport layer	TCP			UDP
Network layer	ICMP			IGMP
	IP			
Data link layer	PPPoE			
	Ethernet			PPP
Physical layer	...			

- Overview of protocols:
  - Hypertext Transfer Protocol (HTTP): used to access various pages on web servers.
  - File Transfer Protocol (FTP): used to transfer data from one host to another.
  - Domain Name Service (DNS): translates domain names of hosts into IP addresses.
  - Transmission Control Protocol (TCP): provides reliable and connection-oriented communication services for applications. Currently, TCP is used by many popular applications.
  - User Datagram Protocol (UDP): provides connectionless communication services, without guaranteeing the reliability of packet transmission.
  - Internet Protocol (IP): encapsulates transport-layer data into data packets and forwards packets from source sites to destination sites. IP provides a connectionless and unreliable service.

## Common TCP/IP Protocols

- The TCP/IP protocol stack defines a set of standard protocols.

Application layer	Telnet HTTP	FTP SMTP	TFTP DNS	SNMP DHCP
Transport layer	TCP			UDP
Network layer	ICMP			IGMP
	IP			
Data link layer	PPPoE			
	Ethernet		PPP	
Physical layer	...			

- Internet Group Management Protocol (IGMP): manages multicast group memberships. Specifically, IGMP sets up and maintains memberships between IP hosts and their directly connected multicast routers.
- Internet Control Message Protocol (ICMP): sends control messages based on the IP protocol and provides information about various problems that may exist in the communication environment. Such information helps administrators diagnose problems and take proper measures to resolve the problems.
- Address Resolution Protocol (ARP): a TCP/IP protocol that discovers the data link layer address associated with a given IP address. It maps IP addresses to MAC addresses, maintains the ARP table that caches the mappings between IP addresses and MAC addresses, and detects IP address conflicts on a network segment.

## TCP

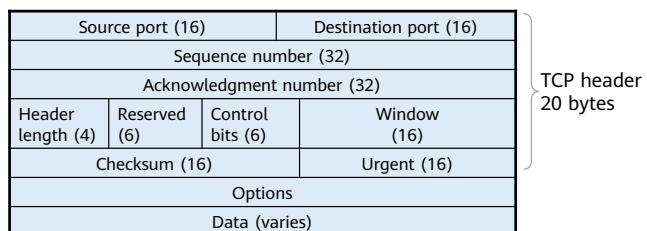
- TCP provides connection-oriented and reliable services for applications.

- Reliability of TCP
  - Connection-oriented transmission

- Maximum segment size (MSS)
- Transmission acknowledgment mechanism

- Checksum of the header and data

- Flow control



- TCP provides reliable and connection-oriented services for applications.
- TCP provides reliability in the following aspects:
  - Connection-oriented transmission: A connection must be established before either side sends data.
  - MSS: limits the maximum length of a TCP packet sent to the receiver.  
When a connection is established, both parties of the connection advertise their MSSs to make full use of bandwidth resources.
  - Transmission acknowledgment mechanism: After the sender sends a data segment, it starts a timer and waits for an acknowledgment from the receiver. If no acknowledgment is received when the timer expires, the sender resends the data segment.
  - Checksum of the header and data: TCP maintains the checksum of the header and data, implementing end-to-end check to verify whether the data changes during transmission. If the checksum of a received segment is incorrect, TCP discards the segment and does not acknowledge the receipt.

of the segment. In this case, TCP starts the retransmission mechanism.

- Flow control: Each party of a TCP connection has a buffer with a fixed size. The receiver allows the sender to send only the data that can be stored in the receive buffer, which prevents buffer overflow caused by the high transmission rate of the sender.

## UDP

- UDP provides connectionless services for applications. Before data transmission, no connection is established between the source and destination ends.
- UDP does not maintain connection states or sending and receiving states. Therefore, a server can transmit the same message to multiple clients at the same time.
- UDP applies to applications that require high transmission efficiency.



- UDP provides connectionless services for applications. That is, no connection needs to be established between the source and destination ends before data transmission. UDP does not maintain connection states or sending and receiving states. Therefore, a server can transmit the same message to multiple clients at the same time.
- UDP applies to applications that require high transmission efficiency or have the reliability guaranteed at the application layer. For example, the Remote Authentication Dial-In User Service (RADIUS) protocol used for authentication and accounting and Routing Information Protocol (RIP) are based on UDP.

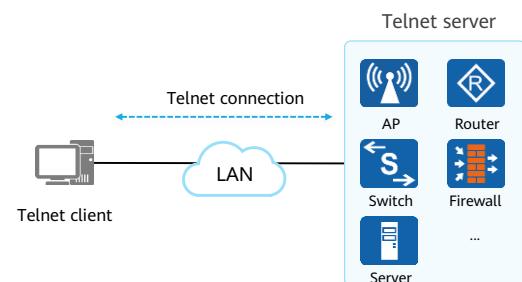
## TCP vs. UDP

TCP	UDP
<ul style="list-style-type: none"><li>• Connection-oriented</li><li>• Reliable transmission with flow and congestion control</li><li>• Header length: 20–60 bytes</li><li>• Applies to applications that require reliable transmission, such as file transfer</li></ul>	<ul style="list-style-type: none"><li>• Connectionless</li><li>• Unreliable transmission, with packet reliability guaranteed by upper-layer applications</li><li>• Short header length of 8 bytes</li><li>• Applies to real-time applications, such as video conferencing</li></ul>

- TCP is reliable, but its reliability mechanism leads to low packet transmission efficiency and high encapsulation overhead.
- UDP is connectionless and unreliable, but its transmission efficiency is higher.

## Telnet

- Telnet provides remote login services on data networks. It allows users to remotely log in to a device from a local PC. Telnet data is transmitted in plaintext.
- A user connects to a Telnet server through a Telnet client program. The commands entered on the Telnet client are executed on the server, as if the commands were entered on the console of the server.

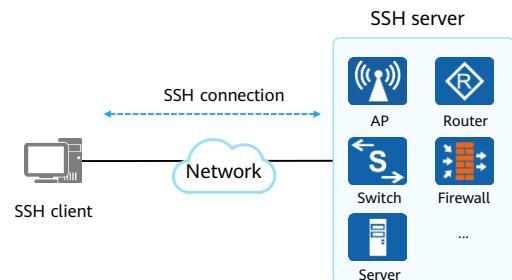


- Telnet enables network administrators to remotely log in to network devices for configuration and management.
- However, Telnet has the following disadvantages:
  - Data is transmitted in plaintext, which does not ensure confidentiality.
  - The authentication mechanism is weak. Users' authentication information is transmitted in plaintext and may be eavesdropped. Telnet supports only the traditional password authentication mode and is vulnerable to attacks.
  - A client cannot truly identify the server. As a result, attackers can use a bogus server to launch attacks.

SSH was designed to resolve the preceding issues.

## SSH

- SSH is a network security protocol that employs encryption and authentication mechanisms to implement services such as secure remote access and file transfer.
- SSH was developed to resolve security issues that Telnet may bring, ensuring secure remote access to network devices.
- SSH uses the client/server architecture and involves three layers: transport layer, authentication layer, and connection layer.



- SSH protocol layers:
  - Transport layer: establishes a secure encryption channel between a client and a server to provide sufficient confidentiality protection for phases that require high data transmission security, such as user authentication and data exchange.
  - Authentication layer: runs over transport-layer protocols and helps a server authenticate login users.
  - Connection layer: divides an encryption channel into several logical channels to run different applications. It runs over authentication-layer protocols and provides services such as session interaction and remote command execution.
- SSH packet exchange consists of the following phases:
  - Connection setup
  - Version negotiation

- Algorithm negotiation
- Key exchange
- User authentication
- Service request
- Data transmission and connection shutdown

## Telnet vs. SSH

Telnet	SSH
<ul style="list-style-type: none"><li>• Data is transmitted in plaintext.</li><li>• Weak authentication mechanism: User authentication information is transmitted in plaintext.</li><li>• Only traditional password authentication is available.</li><li>• A client cannot truly identify a server.</li></ul>	<ul style="list-style-type: none"><li>• Data is transmitted in ciphertext.</li><li>• User authentication information is transmitted in ciphertext.</li><li>• In addition to password authentication, SSH servers support multiple user authentication modes, such as public key authentication that has higher security.</li><li>• Encryption and decryption keys are dynamically generated for communication between the client and server.</li><li>• Provides the server authentication function for clients.</li></ul>

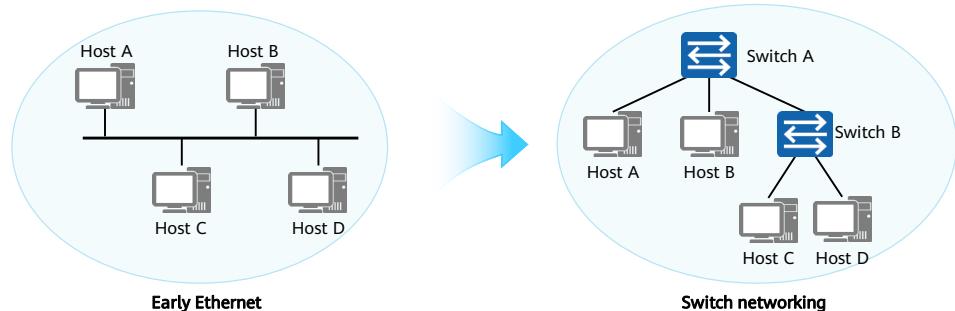
- SSH encrypts data before sending it, ensuring data transmission security. It applies to scenarios where encrypted authentication is required.
- Telnet is still used in tests or scenarios where encryption is not required (such as on a LAN).

# Contents

1. IP Address Basics
2. Introduction to Network Technologies
- 3. Switching Basics**
  - Ethernet Switching Basics
  - VLAN Basics
  - VLAN Basic Configuration
4. Routing Basics

## Ethernet Protocol

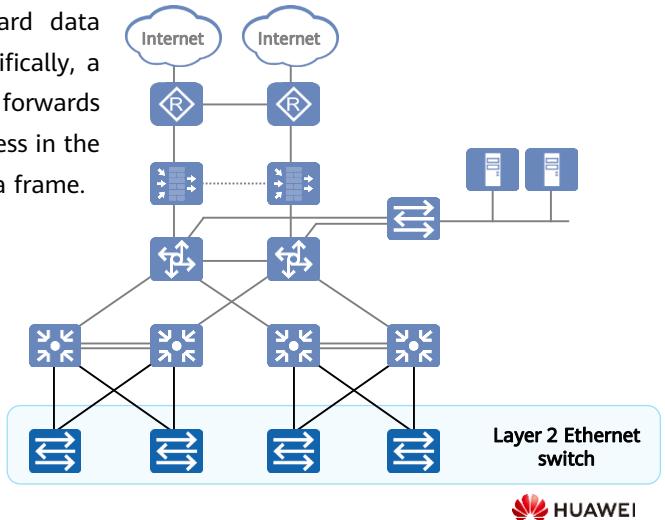
- Ethernet is the most common communication protocol standard used by existing local area networks (LANs). It defines the cable types and signal processing methods that are used on a LAN.



- Early Ethernet:
  - Ethernet networks are broadcast networks established based on the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism. Collisions restrict Ethernet performance. Early Ethernet devices such as hubs work at the physical layer, and cannot confine collisions to a particular scope. This restricts network performance improvement.
- Switch networking:
  - Working at the data link layer, switches are able to confine collisions to a particular scope, thereby helping improve Ethernet performance. Switches have replaced hubs as mainstream Ethernet devices. However, switches do not restrict broadcast traffic on the Ethernet. This affects Ethernet performance.

## Layer 2 Ethernet Switch

- Layer 2 Ethernet switches forward data through Ethernet interfaces. Specifically, a switch performs addressing and forwards data only based on the MAC address in the Layer 2 header of an Ethernet data frame.



42 Huawei Confidential

 HUAWEI

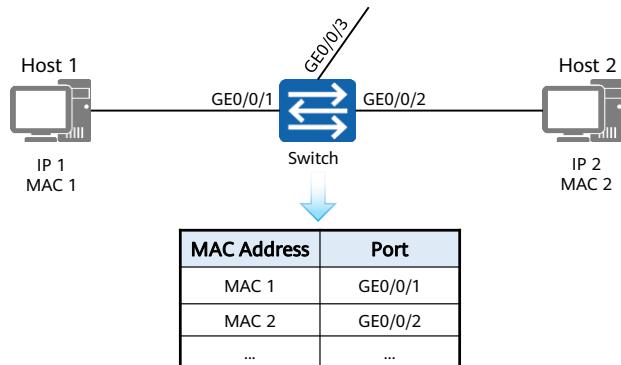
- We have discussed the architecture and composition of a communication network. Layer 2 Ethernet switches are located at the edge of a communication network and function as access devices for user and terminal access.
- Layer 2 Ethernet switch:
  - On a campus network, a switch is the device closest to end users and is used to connect terminals to the campus network. Switches at the access layer are typically Layer 2 switches.
  - A Layer 2 switch works at the second layer (data link layer) of the TCP/IP model and forwards data packets based on MAC addresses.
- Layer 3 Ethernet switch:
  - Routers are required to implement network communication between different LANs. As data communication networks expand and more services emerge on the networks, increasing traffic needs to be transmitted between networks. Routers cannot adapt to this development trend because of their

high costs, low forwarding performance, and small interface quantities.  
New devices capable of high-speed Layer 3 forwarding are required. Layer 3 switches are such devices.

- Note: The switches involved in this course refer to Layer 2 Ethernet switches.

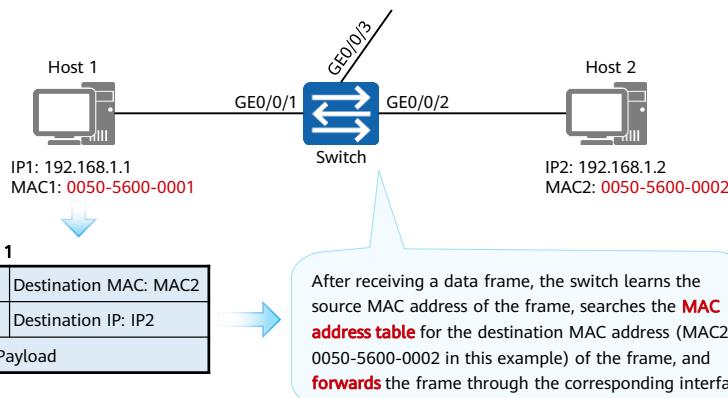
## MAC Address Table

- Each switch has a MAC address table that stores the mappings between MAC addresses and switch interfaces.



- A MAC address table records the mappings between MAC addresses learned by a switch and switch interfaces. When forwarding a data frame, the switch looks up the MAC address table based on the destination MAC address of the frame. If the MAC address table contains an entry mapping the destination MAC address of the frame, the frame is directly forwarded through the outbound interface in the entry. If there is no match of the destination MAC address of the frame in the MAC address table, the switch floods the frame to all interfaces except the interface that receives the frame.

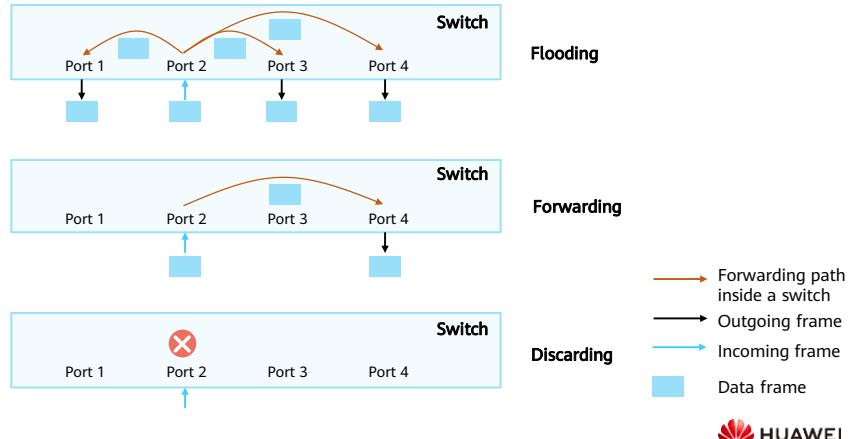
# Working Principles of Switches



- Layer 2 switches work at the data link layer and forward frames based on MAC addresses. Different interfaces on a switch send and receive data independently, and each interface belongs to a different collision domain. This effectively isolates collision domains on the network.
- Layer 2 switches maintain the mappings between MAC addresses and interfaces by learning the source MAC addresses of Ethernet frames in a table called a MAC address table. Layer 2 switches look up the MAC address table to determine the interface to which a frame is forwarded based on the destination MAC address of the frame.

## Three Frame Processing Behaviors of a Switch

- A switch processes the frames entering an interface over a transmission medium in three ways:



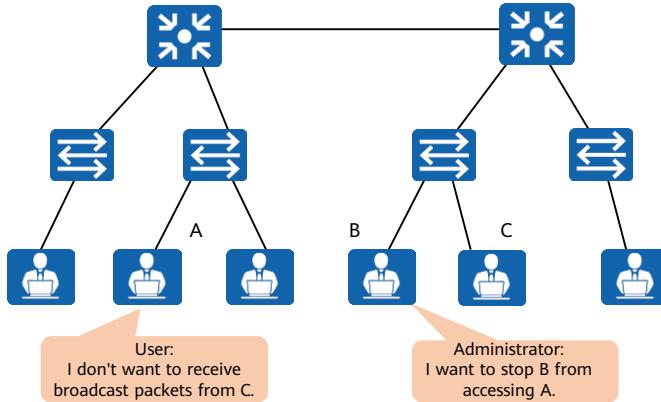
- A switch forwards each frame that enters an interface over a transmission medium, which is also the basic function of a switch.
- A switch processes frames in three ways: flooding, forwarding, and discarding.
  - Flooding:** The switch forwards the frames received from an interface to all other interfaces.
  - Forwarding:** The switch forwards the frames received from an interface to another interface.
  - Discarding:** The switch discards the frames received from an interface.

# Contents

1. IP Address Basics
2. Introduction to Network Technologies
- 3. Switching Basics**
  - Ethernet Switching Basics
  - **VLAN Basics**
  - VLAN Basic Configuration
4. Routing Basics

## Why Do We Need VLANs?

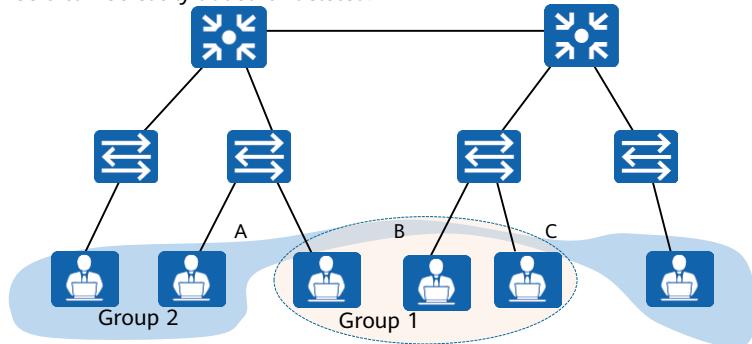
- Broadcast packets have a wide-ranging impact on a network. However, Ethernet has no method for forwarding control.



- Traditional Ethernet switches learn source MAC addresses (MAC addresses of hosts connected to the switch interfaces) of received frames to generate a forwarding table, based on which the switch then forwards frames. All the interfaces can communicate with each other, meaning that maintenance personnel cannot control forwarding between interfaces. Such a network has the following disadvantages:
  - Low network security: The network is prone to attacks because all interfaces can communicate with each other.
  - Low forwarding efficiency: Users may receive a large number of unnecessary packets such as broadcast packets, which consume a lot of bandwidth and host CPU resources.
  - Low service scalability: Network devices process packets on an equal basis and cannot provide differentiated services. For example, Ethernet frames used for network management cannot be preferentially forwarded.

## Objectives of the VLAN Technology

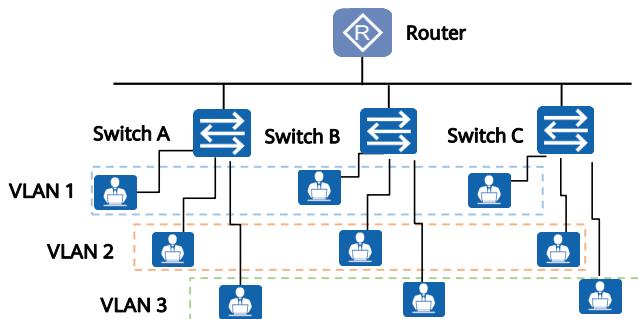
- The Virtual Local Area Network (VLAN) technology divides users into multiple logical groups (networks). Intra-group communication is allowed, whereas inter-group communication is prohibited. Layer 2 unicast, multicast, and broadcast packets can be forwarded only within a group. In addition, group members can be easily added or deleted.



- The VLAN technology provides a management method for controlling the communication between terminals. As shown in the figure above, PCs in Group 1 and PCs in Group 2 cannot communicate with each other.

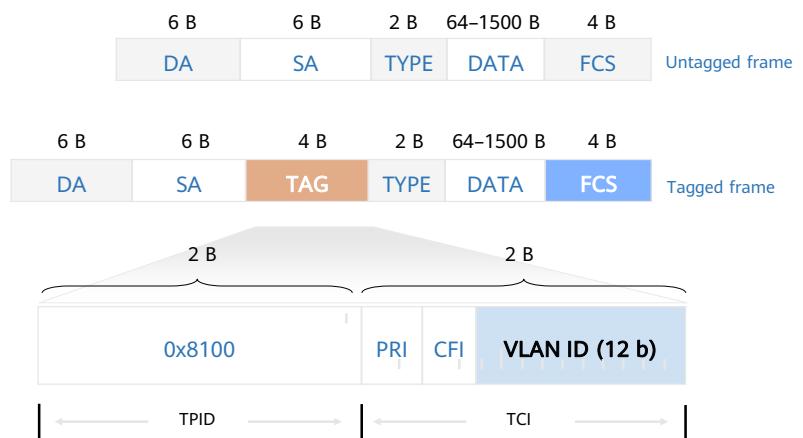
## What Is VLAN?

- The VLAN technology logically divides a physical LAN into multiple VLANs (broadcast domains).



- Hosts within a VLAN can communicate with each other but cannot communicate directly with hosts in other VLANs. This confines broadcast packets within a single VLAN. Inter-VLAN communication is not allowed, which improves network security. For example, if enterprises in the same building establish their own LANs, the cost is high. If enterprises share the same LAN in the building, there may be security risks. In this case, the VLAN technology can be adopted to enable enterprises to share the same LAN while ensuring information security.
- The figure above shows a typical VLAN networking. Three switches are deployed at different locations, for example, on different floors of a building. Each switch is connected to three PCs that belong to different VLANs (for example, VLANs for different enterprises).

## VLAN Frame Format



50 Huawei Confidential

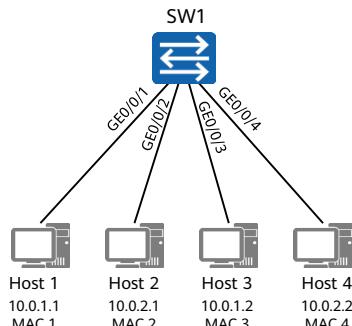


- IEEE 802.1Q adds a 4-byte VLAN tag to an Ethernet frame header.
- Tag Protocol Identifier (TPID): identifies a frame as an 802.1Q-tagged frame. This field is of 2 bytes and has a fixed value of 0x8100.
- Tag Control Information (TCI): indicates the control information of an Ethernet frame. This field is of 2 bytes.
  - Priority: identifies the priority of an Ethernet frame. This field is of 3 bits. The value of this field ranges from 0 to 7, providing differentiated forwarding services.
  - Canonical Format Indicator (CFI): indicates the bit order of address information in an Ethernet frame. This field is used in token ring or FDDI source-routed MAC methods and is of 1 bit.
  - VLAN Identifier (VLAN ID): controls the forwarding of Ethernet frames based on the VLAN configuration on a switch interface. This field is of 12 bits, with its value ranging from 0 to 4095.

- Since VLAN tags are adopted, Ethernet frames are classified as untagged frames (without 4-byte VLAN tags) or tagged frames (with 4-byte VLAN tags).
- In this course, only the VLAN ID field is discussed.

## VLAN Assignment Methods

- How are VLANs assigned on a network?



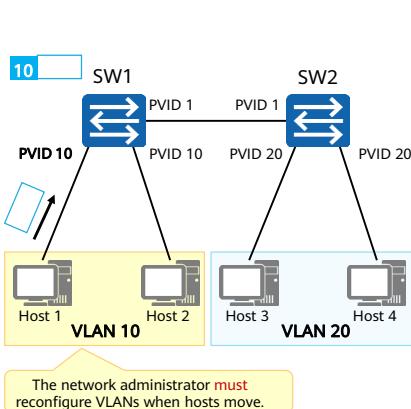
VLAN Assignment Method	VLAN 10	VLAN 20
Interface-based	GE0/0/1, GE0/0/3	GE0/0/2, GE0/0/4
MAC address-based	MAC 1, MAC 3	MAC 2, MAC 4
IP subnet-based	10.0.1.*	10.0.2.*
Protocol-based	IP	IPv6
Policy-based	10.0.1.* + GE0/0/1 + MAC 1	10.0.2.* + GE0/0/2 + MAC 2

- PCs send only untagged frames. After receiving such an untagged frame, a switch that supports the VLAN technology needs to assign the frame to a specific VLAN based on certain rules.
- Available VLAN assignment methods are as follows:
  - Interface-based assignment: assigns VLANs based on switch interfaces.
    - A network administrator preconfigures a port VLAN ID (PVID) for each switch interface. When an untagged frame arrives at an interface of a switch, the switch tags the frame with the PVID of the interface. The frame is then transmitted in the specified VLAN.
  - MAC address-based assignment: assigns VLANs based on the source MAC addresses of frames.
    - A network administrator preconfigures the mapping between MAC addresses and VLAN IDs. After receiving an untagged frame, a switch tags the frame with the VLAN ID mapping the source MAC address of the frame. The frame is then transmitted in the specified VLAN.

- IP subnet-based assignment: assigns VLANs based on the source IP addresses and subnet masks of frames.
  - A network administrator preconfigures the mapping between IP addresses and VLAN IDs. After receiving an untagged frame, a switch tags the frame with the VLAN ID mapping the source IP address of the frame. The frame is then transmitted in the specified VLAN.

- Protocol-based assignment: assigns VLANs based on the protocol (suite) types and encapsulation formats of frames.
  - A network administrator preconfigures the mapping between protocol (suite) types and VLAN IDs. After receiving an untagged frame, a switch tags the frame with the VLAN ID mapping the protocol (suite) type of the frame. The frame is then transmitted in the specified VLAN.
- Policy-based assignment: assigns VLANs based on a specified policy, which means VLANs are assigned based on a combination of interfaces, MAC addresses, and IP addresses.
  - A network administrator preconfigures a policy. After receiving an untagged frame that matches the policy, a switch adds a specified VLAN tag to the frame. The frame is then transmitted in the specified VLAN.

# Interface-based VLAN Assignment



## Interface-based VLAN assignment

### • Principles

- VLANs are assigned based on interfaces.
- A network administrator preconfigures a **PVID** for each switch interface to assign each interface to the VLAN corresponding to the PVID.
- After an interface receives an untagged frame, the switch adds a tag carrying the PVID of the interface to the frame. The frame is then transmitted in the specified VLAN.

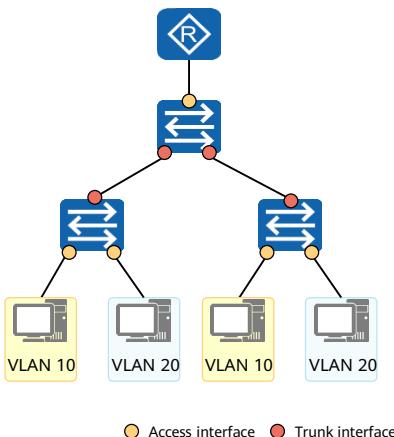
### • PVID (Port VLAN ID)

- Default VLAN ID of an interface
- Value range: 1–4094

- Assignment rule:
  - VLAN IDs are configured on physical interfaces of a switch. All PC-sent untagged frames arriving at a physical interface are assigned to the VLAN corresponding to the PVID configured on the interface.
- Characteristics:
  - This VLAN assignment method is simple, intuitive, and easy to implement. Currently, it is the most widely used VLAN assignment method.
  - When a PC is connected to another switch interface, the frames sent by the PC may be assigned to a different VLAN.
- PVID: default VLAN ID
  - Each switch interface must be configured with a PVID. All untagged frames arriving at a switch interface are assigned to the VLAN corresponding to the PVID configured on the interface.

- The default PVID is 1.

# VLAN Interface Types



Interface type
<b>Access interface</b> An access interface is used to connect a switch to a terminal, such as a PC or server. In general, the NICs on such terminals receive and send only untagged frames. An access interface can be added to only one VLAN.
<b>Trunk interface</b> A trunk interface is used to connect a switch to another switch or a sub-interface on a device such as a router or firewall. This type of interface allows frames that belong to multiple VLANs to pass through and differentiates the frames using the 802.1Q tag.
<b>Hybrid interface</b> Similar to a trunk interface, a hybrid interface also allows frames that belong to multiple VLANs to pass through and differentiates the frames using the 802.1Q tag. You can determine whether to allow a hybrid interface to send frames that belong to one or multiple VLANs VLAN-tagged.

- The interface-based VLAN assignment method varies according to the switch interface type.
- Access interface
  - An access interface often connects to a terminal (such as a PC or server) that cannot identify VLAN tags, or is used when VLANs do not need to be differentiated.
- Trunk interface
  - A trunk interface often connects to a switch, router, AP, or voice terminal that can accept and send both tagged and untagged frames.
- Hybrid interface
  - A hybrid interface can connect to a terminal (such as a PC or server) that cannot identify VLAN tags or to a switch, router, AP, or voice terminal that can accept and send both tagged and untagged frames.

- By default, hybrid interfaces are used on Huawei devices.

# Contents

1. IP Address Basics
2. Introduction to Network Technologies
- 3. Switching Basics**
  - Ethernet Switching Basics
  - VLAN Basics
    - VLAN Basic Configuration
4. Routing Basics

# Basic VLAN Configuration Commands

- Create VLANs.

```
[Huawei] vlan vlan-id
```

- Create a VLAN and enter the VLAN view, or enter the view of an existing VLAN.
- The value of *vlan-id* is an integer that ranges from 1 to 4094.

```
[Huawei] vlan batch { vlan-id1 [ to vlan-id2 ] }
```

Create VLANs in a batch.

- **batch**: creates VLANs in a batch.
- *vlan-id1*: specifies the start VLAN ID.
- *vlan-id2*: specifies the end VLAN ID.

- The **vlan** command creates a VLAN and displays the VLAN view. If the VLAN to be created exists, the VLAN view is displayed directly.
- The **undo vlan** command deletes a VLAN.
- By default, all interfaces belong to the default VLAN, that is, VLAN 1.
  - Commands:
    - **vlan *vlan-id***
      - *vlan-id*: specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
    - **vlan batch { *vlan-id1* [ to *vlan-id2* ] }**
      - **batch**: creates VLANs in a batch.
      - *vlan-id1* to *vlan-id2*: specifies the IDs of VLANs to be created in a batch.
        - *vlan-id1* specifies the start VLAN ID.
        - *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2*

must be greater than or equal to that of *vlan-id1*. *vlan-id1* and *vlan-id2* identify a VLAN range.

- If **to** *vlan-id2* is not specified, the VLAN specified by *vlan-id1* is created.
- The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

## Basic Access Interface Configuration Commands

- Set the interface type.

```
[Huawei-GigabitEthernet0/0/1] port link-type access
```

- In the interface view, set the link type of the interface to access.

- Configure the default VLAN of the access interface.

```
[Huawei-GigabitEthernet0/0/1] port default vlan vlan-id
```

- In the interface view, configure the default VLAN of the interface and add the interface to the VLAN.
  - *vlan-id*: specifies the default VLAN ID. The value is an integer that ranges from 1 to 4094.

# Basic Trunk Interface Configuration Commands

- Set the interface type.

```
[Huawei-GigabitEthernet0/0/1] port link-type trunk
```

- In the interface view, set the link type of the interface to trunk.

- Add the trunk interface to specified VLANs.

```
[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] } | all }
```

- In the interface view, add the trunk interface to specified VLANs.

- (Optional) Configure the default VLAN of the trunk interface.

```
[Huawei-GigabitEthernet0/0/1] port trunk pvid vlan vlan-id
```

- In the interface view, configure the default VLAN of the trunk interface.

- Command: `port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] } | all }`
  - *vlan-id1* [ to *vlan-id2* ]: specifies the VLANs to which the trunk interface is added.
    - *vlan-id1* specifies the start VLAN ID.
    - *to vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
  - **all**: adds the trunk interface to all VLANs.
- Command: `port trunk pvid vlan vlan-id`
  - *vlan-id*: specifies the default VLAN ID of the trunk interface. The value is an integer that ranges from 1 to 4094.

# Basic Hybrid Interface Configuration Commands

- Set the interface type.

```
[Huawei-GigabitEthernet0/0/1] port link-type hybrid
```

- In the interface view, set the link type of the interface to hybrid.

- Add the hybrid interface to specified VLANs.

```
[Huawei-GigabitEthernet0/0/1] port hybrid untagged vlan { { vlan-id1 [ to vlan-id2 ] } | all }
```

- In the interface view, add the hybrid interface to specified VLANs. Frames that belong to these VLANs then pass through the hybrid interface in untagged mode.

```
[Huawei-GigabitEthernet0/0/1] port hybrid tagged vlan { { vlan-id1 [ to vlan-id2 ] } | all }
```

- In the interface view, add the hybrid interface to specified VLANs. Frames that belong to these VLANs then pass through the hybrid interface in tagged mode.

- (Optional) Configure the default VLAN of the hybrid interface.

```
[Huawei-GigabitEthernet0/0/1] port hybrid pvid vlan vlan-id
```

- In the interface view, configure the default VLAN of the hybrid interface.

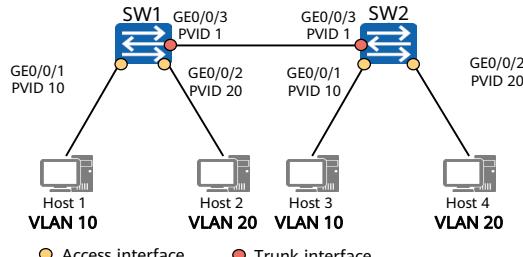
- Command: `port hybrid untagged vlan { { vlan-id1 [ to vlan-id2 ] } | all }`
  - *vlan-id1* [ to *vlan-id2* ]: specifies the VLANs to which the hybrid interface is added.
    - *vlan-id1* specifies the start VLAN ID.
    - **to *vlan-id2*** specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
  - **all**: adds the hybrid interface to all VLANs.
- Command: `port hybrid tagged vlan { { vlan-id1 [ to vlan-id2 ] } | all }`
  - *vlan-id1* [ to *vlan-id2* ]: specifies the VLANs to which the hybrid interface is added.
    - *vlan-id1* specifies the start VLAN ID.
    - **to *vlan-id2*** specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are integers that range from 1

to 4094.

- **all**: adds the hybrid interface to all VLANs.
- Command: port hybrid pvid vlan *vlan-id*
  - *vlan-id*: specifies the default VLAN ID of the hybrid interface. The value is an integer that ranges from 1 to 4094.

## Configuration Example: Configuring Interface-based VLAN Assignment

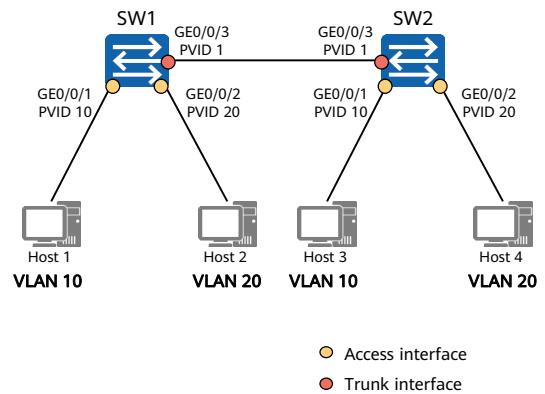
- Networking requirements
  - There are many users connected to an enterprise's switches. Currently, users of the same service access the enterprise network through different switches. To ensure communication security, the enterprise requires that users with the same service can directly communicate only with each other.
  - To meet this requirement, configure interface-based VLAN assignment on the switches and add interfaces connecting users with the same service to the same VLAN. In this way, users in the same VLAN can directly communicate only with each other at Layer 2.



# Creating VLANs

Create VLANs:

```
[SW1] vlan 10  
[SW1-vlan10] quit  
[SW1] vlan 20  
[SW1-vlan20] quit  
  
[SW2] vlan batch 10 20
```



# Configuring Access and Trunk Interfaces

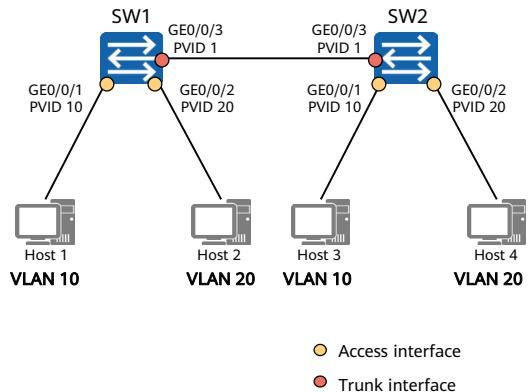
Configure access interfaces and add the interfaces to corresponding VLANs.

```
[SW1] interface GigabitEthernet 0/0/1  
[SW1-GigabitEthernet0/0/1] port link-type access  
[SW1-GigabitEthernet0/0/1] port default vlan 10
```

```
[SW1] interface GigabitEthernet 0/0/2  
[SW1-GigabitEthernet0/0/2] port link-type access  
[SW1] vlan 20  
[SW1-vlan20] port GigabitEthernet0/0/2  
[SW1-vlan20] quit
```

Configure a trunk interface and configure allowed VLANs for the interface.

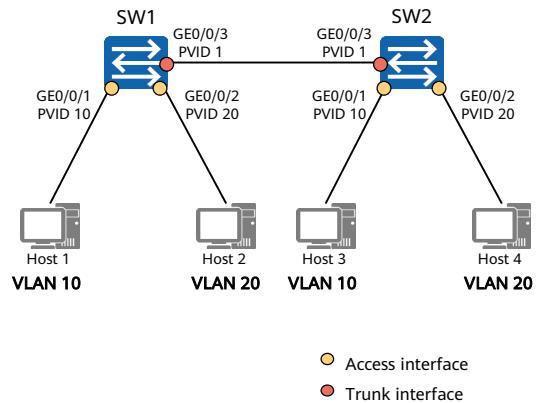
```
[SW1] interface GigabitEthernet 0/0/3  
[SW1-GigabitEthernet0/0/3] port link-type trunk  
[SW1-GigabitEthernet0/0/3] port trunk pvid vlan 1  
[SW1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
```



Note: The configuration on SW2 is similar to that on SW1.

## Verifying the Configuration

```
[SW1]display vlan
The total number of vlans is: 3
-----
U: Up; D: Down; TG: Tagged; UT:
Untagged;
MP: Vlan-mapping; ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;
-----
VID      Type      Ports
-----
1        common    UT:GE0/0/3(U) ...
10       common    UT:GE0/0/1(U)
                  TG:GE0/0/3(U)
20       common    UT:GE0/0/2(U)
                  TG:GE0/0/3(U)
```



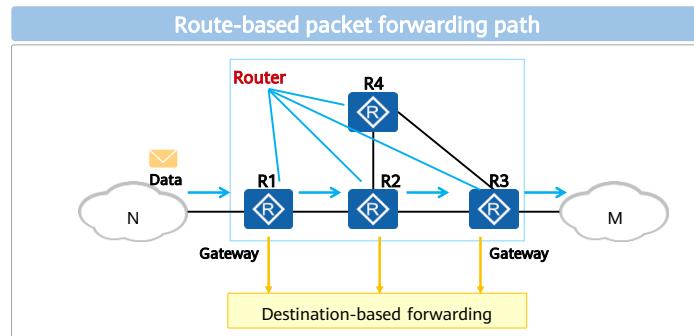
- The **display vlan** command displays information about VLANs.
- Description of the command output:
  - **Tagged/Untagged Port**: interfaces that are manually added to a VLAN in tagged or untagged mode.
  - **VID or VLAN ID**: VLAN ID.
  - **Type or VLAN Type**: VLAN type. The value **common** indicates a common VLAN.
  - **Ports**: interfaces added to a VLAN.

# Contents

1. IP Address Basics
2. Introduction to Network Technologies
3. Switching Basics
- 4. Routing Basics**
  - Basic Routing Principles
    - Static and Default Routes

## Routes

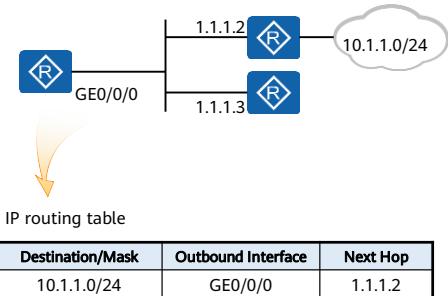
- Routes are the path information that is used to guide packet forwarding.
- A routing device is one that forwards packets to a destination network segment based on routes. The most common routing device is a router.
- A routing device maintains an IP routing table that stores routing information.



- A gateway and an intermediate node (a router) select a proper path according to the destination address of a received IP packet, and forward the packet to the next router. The last-hop router on the path performs Layer 2 addressing and forwards the packet to the destination host. This process is called route-based forwarding.
- The intermediate node selects the best path from its IP routing table to forward packets.
- A routing entry contains a specific outbound interface and next hop, which are used to forward IP packets to the corresponding next-hop device.

# Routing Information

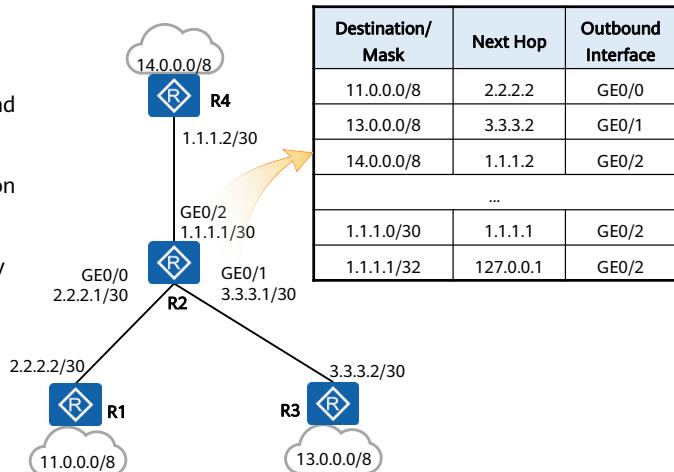
- A route contains the following information:
  - Destination network: identifies a destination network segment.
  - Mask: identifies a network segment together with a destination IP address.
  - Outbound interface: indicates the interface through which a data packet is sent out of the local router.
  - Next hop: indicates the next-hop address used by the router to forward the data packet to the destination network segment.
- The information identifies the destination network segment and specifies the path for forwarding data packets.



- Based on the information contained in a route, a router can forward IP packets to the destination network segment along the corresponding path.
- The destination address and mask identify the destination address of an IP packet. After an IP packet matches a specific route, the router determines the forwarding path according to the outbound interface and next hop of the route.
- The next-hop device for forwarding the IP packet cannot be determined based only on the outbound interface. Therefore, the next-hop device address must be specified.

## Routing Table

- A router discovers routes using multiple methods.
- A router selects the optimal route and installs it in its IP routing table.
- A router forwards IP packets based on routes in the IP routing table.
- Routers manage path information by managing their IP routing tables.



- A router forwards packets based on its IP routing table.
- An IP routing table contains many routing entries.
- An IP routing table contains only optimal routes.
- A router manages routing information by managing the routing entries in its IP routing table.

## Checking the IP Routing Table

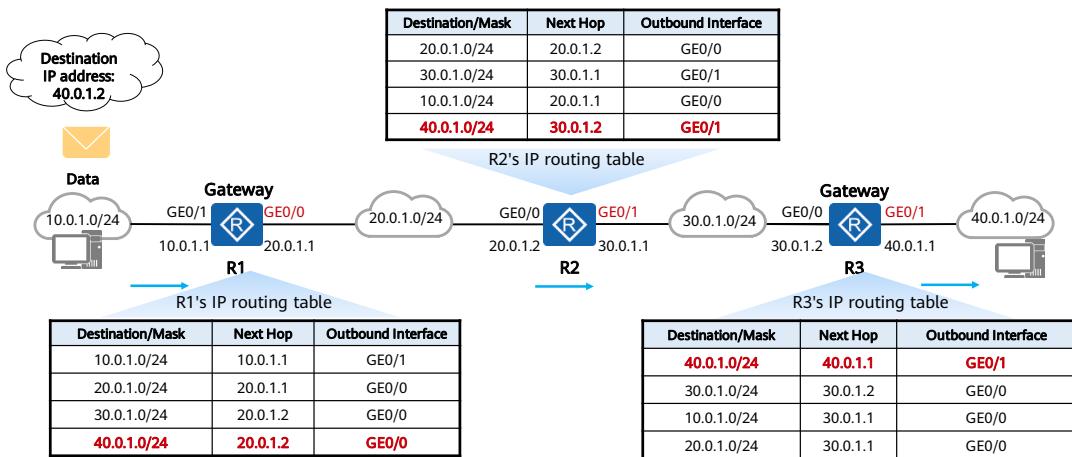
<Huawei> display ip routing-table Route Flags: R - relay, D - download to fib						
Routing Tables: Public		Destinations: 6 Routes: 6				
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
1.1.1.1/32	Static	60	0	D	0.0.0.0	NULL0
2.2.2.2/32	Static	60	0	D	100.0.0.2	Vlanif100
100.0.0.0/24	Direct	0	0	D	100.0.0.1	Vlanif100
100.0.0.1/32	Direct	0	0	D	127.0.0.1	Vlanif100
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0

Destination network address/Mask    Protocol type    Route preference    Cost (metric)    Flag    Next-hop IP address    Outbound interface

- Destination/Mask: indicates the destination network address and mask of a specific route. The network segment address of a destination host or router is obtained through the AND operation on the destination address and mask. For example, if the destination address is 1.1.1.1 and the mask is 255.255.255.0, the IP address of the network segment to which the host or router belongs is 1.1.1.0.
- Proto (Protocol): indicates the protocol type of the route, that is, the protocol through which a router learns the route.
- Pre (Preference): indicates the routing protocol preference of the route. There may be multiple routes to the same destination, which have different next hops and outbound interfaces. These routes may be discovered by different routing protocols or manually configured. A router selects the route with the highest preference (with the lowest preference value) as the optimal route.
- Cost: indicates the cost of the route. When multiple routes to the same destination have the same preference, the route with the lowest cost is selected as the optimal route.

- NextHop: indicates the local router's next-hop address of the route to the destination network. This field specifies the next-hop device to which packets are forwarded.
- Interface: indicates the outbound interface of the route. This field specifies the local interface through which the local router forwards packets.

## Route-based Forwarding Process



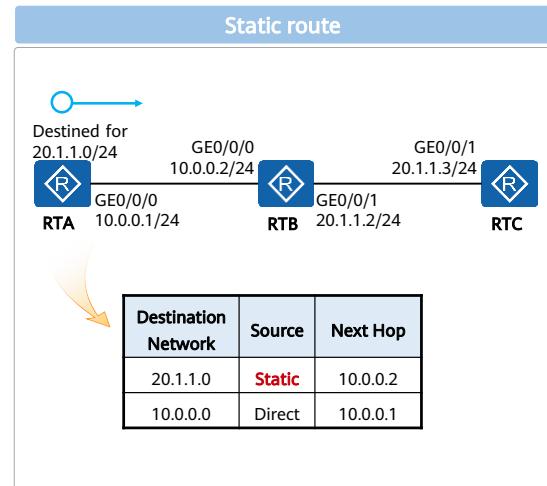
- The IP packets from 10.0.1.0/24 need to reach 40.0.1.0/24. These packets arrive at the gateway R1, which then searches its IP routing table for the next hop and outbound interface and forwards the packets to R2. After the packets reach R2, R2 forwards the packets to R3 by searching its IP routing table. After receiving the packets, R3 searches its IP routing table, finding that the destination IP address of the packets belongs to the network segment where a local interface resides. Therefore, R3 directly forwards the packets to the destination network segment 40.0.1.0/24.

# Contents

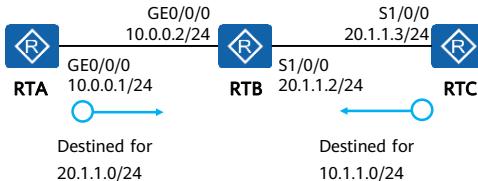
1. IP Address Basics
2. Introduction to Network Technologies
3. Switching Basics
- 4. Routing Basics**
  - Basic Routing Principles
  - Static and Default Routes

## Introduction to Static Routes

- Static routes are manually configured by network administrators, have low system requirements, and apply to simple, stable, and small networks.
- However, static routes cannot automatically adapt to network topology changes and so require manual intervention.
- Packets destined for 20.1.1.0/24 do not match the direct route in RTA's IP routing table. In this case, a static route needs to be manually configured so that the packets sent from RTA to 20.1.1.0/24 can be forwarded to the next hop 10.0.0.2.



## Configuration Example



Configure RTA.

```
[RTA] ip route-static 20.1.1.0 255.255.255.0 10.0.0.2
```

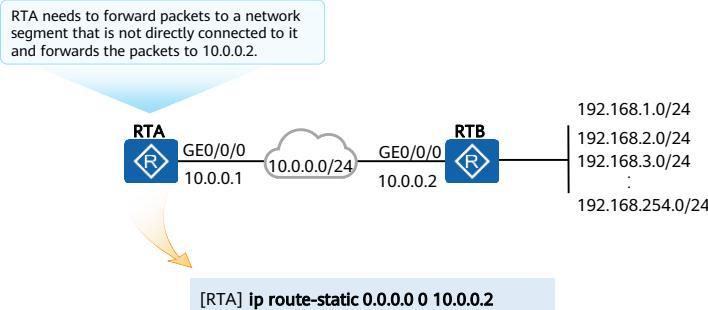
Configure RTC.

```
[RTC] ip route-static 10.0.0.0 255.255.255.0 S1/0/0
```

- Configure static routes on RTA and RTC for communication between 10.0.0.0/24 and 20.1.1.0/24.
- Packets are forwarded hop by hop. Therefore, all the routers along the path from the source to the destination must have routes destined for the destination.
- Data communication is bidirectional. Therefore, both forward and return routes must be available.

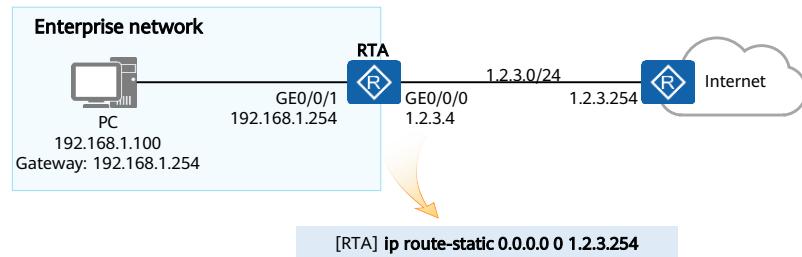
## Default Route

- Default routes are used only when packets to be forwarded do not match any routing entry in an IP routing table.
- In an IP routing table, a default route is the route to network 0.0.0.0 (with the mask 0.0.0.0), namely, 0.0.0.0/0.



## Application Scenarios of Default Routes

- Default routes are typically used at the egress of an enterprise network. For example, you can configure a default route on an egress device so that the device forwards IP packets destined for any address on the Internet.



## Summary

- In this course, we have learned the composition of IP addresses, subnetting, basic principles of network communication, and basic operations and application scenarios of common network protocols. In the following course, we will learn operating system basics. Stay tuned.

# Quiz

1. Which of the following are functions of firewalls?
  - A. Isolating networks of different security levels
  - B. Authenticating user identities
  - C. Implementing NAT
  - D. Performing route calculation
2. Default routes are typically used at the egress of an enterprise network. For example, you can configure a default route on an egress device so that the device forwards IP packets destined for any address on the Internet.
  - A. True
  - B. False

- Answers:

- ABCD
  - A

# Recommendations

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

## Acronyms and Abbreviations

- ARP: Address Resolution Protocol
- DNS: Domain Name Service
- FTP: File Transfer Protocol
- HTTP: Hypertext Transfer Protocol
- ICMP: Internet Control Message Protocol
- IGMP: Internet Group Management Protocol
- IP: Internet Protocol
- LAN: Local Area Network
- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- VLAN: Virtual Local Area Network
- VLSM: Variable Length Subnet Mask

# 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.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



# Operating System Basics



# Foreword

- The operating system (OS) plays an important role in the interaction between the user and the computer. But what exactly is an OS? What are the types of OSs? What are the basic commands of the Linux system? This course explores these questions, and more, to help you better understand OSs.

# Objectives

- Upon completion of this course, you will understand:
  - The definition and components of OSs.
  - Different types of OSs.
  - Basic Linux operations.

# Contents

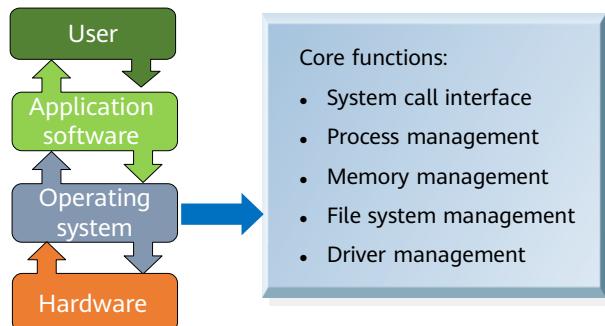
## **1. Operating System Basics**

- Definition
  - Components of an OS
  - Different Types of OSs

## **2. Linux Basics**

# Operating System Definition and Functions

- An operating system (OS) is a computer program (system software) that manages and controls computer hardware and software resources.



- An operating system is a special computer program that controls the computer, connects the computer and the user, and coordinates and manages hardware resources, including the CPU, drive, memory, and printer. These resources are required for running programs.
- Mainstream OSs:
  - From the perspective of application field, OSs are classified into the following types:
    - Desktop OS, server OS, host OS, and embedded OS.
  - Based on whether an OS is open source, it is classified as:
    - Open source OS (Linux and Unix) or close source OS (Windows and Mac OS).

# Contents

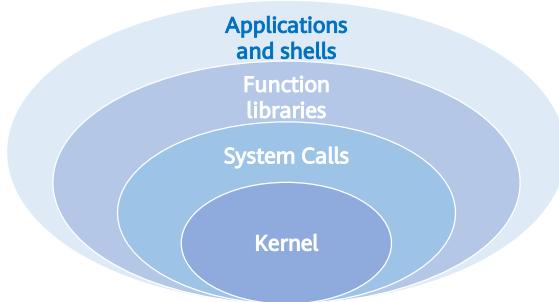
## **1. Operating System Basics**

- Definition
- Components of an OS
- Different Types of OSs

## **2. Linux Basics**

# Components of an Operating System

- From the perspective of users, an OS consists of a kernel and various applications, that is, the kernel space and user space.
- The user space is where upper-layer applications run.
- The kernel is essentially a software program used to manage computer hardware resources and provide a system call interface to run upper-layer application programs.



- System calls: The execution of applications depends on resources provided by the kernel, including the CPU, storage, and I/O resources. To enable upper-layer applications to access these resources, the kernel must provide an access interface, that is, the system call interface.
- Library functions: System calls are encapsulated as library functions to provide simple service logic interfaces to users. Simple access to system resources can be completed using system calls. Library functions allow for complex access to system resources.
- Shell: A shell is a special application program, which is also called the command line interface. It is a command interpreter in essence. It can execute texts (scripts) that comply with the shell syntax. Some shell script statements encapsulate system calls for convenient use.

- The kernel controls hardware resources, manages OS resources, and provides a system call interface for applications.
  - Process scheduling and management: The kernel creates and destroys processes and handles their input and output.
  - Memory management: The kernel creates a virtual address space for all processes based on limited available resources.
  - File system management: Linux is based on the concept of file system to a large extent. Almost anything in Linux can be seen as a file. The kernel builds a structured file system on top of unstructured hardware.
  - Device driver management: Drivers of all peripherals in the system, such as hard drives, keyboards, and tape drives, are embedded in the kernel.
  - Network resource management: All routing and address resolution operations are performed in the kernel.
- Summary: User-mode applications can access kernel-mode resources using the following:
  - System calls
  - Shell scripts
  - Library functions

# Contents

## **1. Operating System Basics**

- Definition
- Components of an OS
- Different Types of OSs

## **2. Linux Basics**

## Common Server OSs

UNIX

A multi-user and multi-process OS. It supports large-scale file system services and data service applications, provides powerful functions, and ensures high stability and security.

**Common Unix OSs:**  
HP-UX, IBM AIX, Solaris, and A/UX.

GNU/  
Linux

Linux is a general term for Unix-like OSs. Linux runs with high security and stability and has a complete permission control mechanism.

**Common Linux OSs:**  
SUSE Linux, Kylin, Red Flag Linux, CentOS, RHEL, and openEuler.

Windows

Windows Server is a server OS released by Microsoft. It is mainly used on servers and provides a user-friendly GUI.

**Common Windows Server versions:**  
2000, 2003, 2008, 2012, 2016, and 2019.

- Relationship between Linux and Unix:
  - Linux is a Unix-like OS with optimized functions and user experience. Linux mimics Unix in terms of appearance and interaction.
  - The Linux kernel was initially written by Linus Torvalds for a hobby when he was studying at the University of Helsinki. Frustrated by MINIX, a Unix-like OS for educational purposes, he decided to develop his own OS. The first version was released in September 1991 with only 10,000 lines of code.
  - Unix systems are usually compatible only with specific hardware. This means that most Unix systems such as AIX and HP-UX cannot be installed on x86 servers or PCs. On the contrary, Linux can run on various hardware platforms.
  - Unix is commercial software, while Linux is open source and free of charge.
- The GNU Project:
  - The GNU Project was publicly announced on September 27, 1983 by Richard Stallman, aiming at building an OS composed wholly of free software.
  - GNU is a recursive acronym for "GNU's Not Unix". Linux provides a kernel, and GNU provides a large amount of free software to enrich the various applications run on the kernel.

# Contents

## 1. Operating System Basics

### 2. Linux Basics

- Introduction to Linux
  - Introduction to openEuler
  - Introduction to File Systems on openEuler
  - Basic openEuler Operations

## Features of Linux

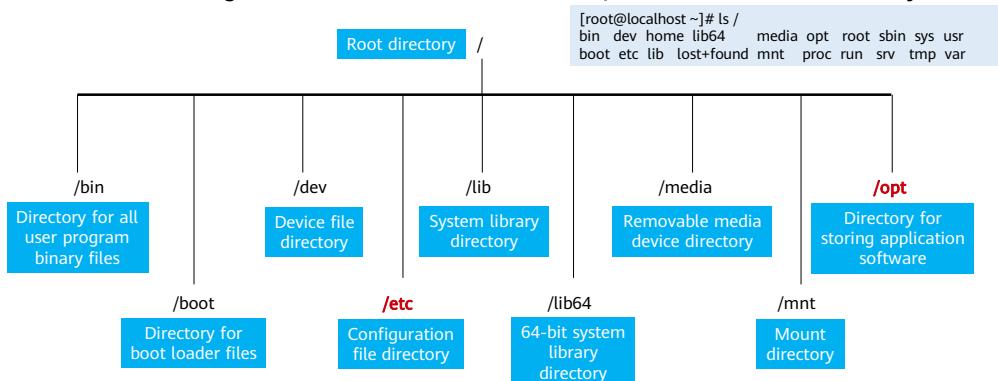
- Multi-platform design
  - Linux can run on multiple hardware platforms. The Linux kernel is also used in embedded systems that run on devices such as handheld computers and set-top boxes.
- Multi-user and multitasking
  - System resources can be used by different users. Multiple programs can run simultaneously and independently.
- Free to use
  - The source code of Linux is available for free. Users can edit and modify the source code as required.
- Fully compatible with the POSIX.1 standard
- Inherits the design concept of Unix
  - Everything is a file.

- The Portable Operating System Interface (POSIX) is a family of standards specified by IEEE. POSIX defines the application programming interfaces (APIs) of software runs on Unix. The family of POSIX standards is formally designated as IEEE 1003 and the ISO/IEC standard number is ISO/IEC 9945. The name of POSIX consists of the abbreviation of Portable Operating System Interface and an X that indicates the inheritance of Unix APIs.
- Linux is a popular multitasking and multi-user OS with the following features:
  - Multitasking: Linux is a multitasking operating system that allows multiple tasks to run at the same time. DOS is a single-task OS and cannot run multiple tasks at the same time. When the system executes multiple tasks, the CPU executes only one task at a time. Linux divides the CPU time into time slices and allocates them to multiple processes. The CPU runs so quickly that all programs (processes) seem to be running at the same time from the user's perspective.
  - Multi-user: Linux is a multi-user OS that allows multiple users to use it at the same time. In Linux, each user runs their own or public programs as if they had a separate machine. DOS is a single-user OS and allows only one user to use it at a time.
  - Pipeline: Linux allows the output of a program to be used as the input of the next program. Multiple programs are chained together as a pipeline. By combining simple tasks, you can complete complex tasks, improving the operation convenience. Later versions of DOS learned from Linux and implemented this mechanism.
  - Powerful shells: Shells are the command interpreters of Linux. Linux provides multiple powerful shells, each of which is an interpreted high-level

language. Users can create numerous commands through programming.

# Linux File Directory Structure

- Linux OS adopts "Everything is a file" design.
- Linux directories are organized in a tree structure, where `/` indicates the root directory.



- The core philosophy of Linux is "everything is a file", which means that all files, including directories, character devices, block devices, sockets, printers, processes, threads, and pipes, can be operated, read, and written by using functions such as `fopen()`, `fclose()`, `fwrite()`, and `fread()`.
- After logging in to the system, enter the `ls /` command in the current command window. The command output similar to the figure is displayed. The directories are described as follows:
  - `/bin`: short for binary. This directory stores the frequently used commands.
  - `/boot`: stores some core files used for booting the Linux OS, including some links and images.
  - `/dev`: short for device. This directory stores peripheral device files of Linux. The method of accessing devices on Linux is the same as that of accessing files.
  - `/etc`: stores all configuration files and subdirectories required for system management.
  - `/lib`: stores basic shared libraries of the system. A library functions similarly to a dynamic link library (DLL) file on Windows. Almost all applications need to use these shared libraries.
  - `/mnt`: temporary mount point for other file systems. You can mount the CD-ROM drive to `/mnt` and then go to this directory to view the contents in the CD-ROM.
  - `/opt`: stores additional software installed on the host. For example, if you install an Oracle database, you can save the installation package to this directory. By default, this directory is empty.

# Contents

## 1. Operating System Basics

### **2. Linux Basics**

- Introduction to Linux
- **Introduction to openEuler**
- Introduction to File Systems on openEuler
- Basic openEuler Operations

## Background of openEuler

- EulerOS is a server OS that runs on the Linux kernel and supports processors of multiple architectures, such as x86 and ARM. It is ideal for database, big data, cloud computing, and artificial intelligence (AI) scenarios.
- Over the past decade, EulerOS has interconnected with various Huawei products and solutions. It is respected for its security, stability, and efficiency.
- Cloud computing, in addition to Kunpeng processors, has sparked the growth of EulerOS to become the most powerful software infrastructure in the Kunpeng ecosystem.
- To develop the Kunpeng ecosystem and build prosperity of the computing industry in China and around the world, the open source version of EulerOS was officially released as openEuler at the end of 2019.



## Introduction to openEuler

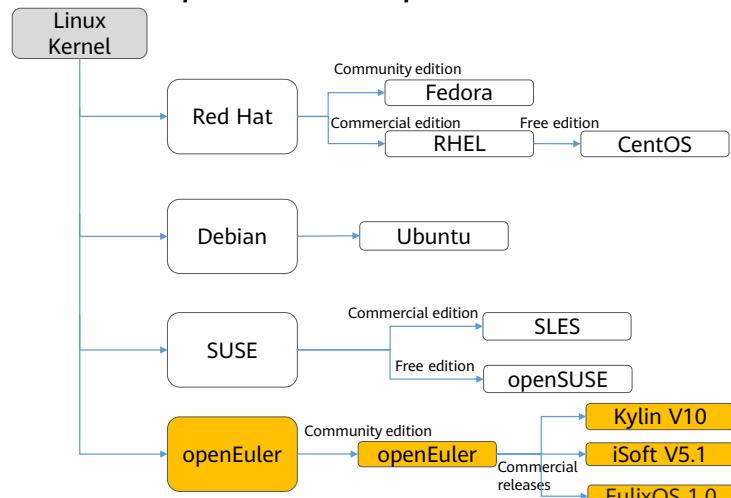
- openEuler is a free open source Linux distribution that supports multiple processor architectures including x86, ARM, and RISC-V.
- All developers, enterprises, and business organizations can simply use the openEuler community version, or use it to build, develop, and release their own OS versions.

<https://openeuler.org/>

<https://gitee.com/openeuler/>



## Relationship Between openEuler and Mainstream OSs



- The upstream community of openEuler, SUSE, Debian, and Red Hat is the kernel community [www.kernel.org](http://www.kernel.org).
- The openEuler community releases free long-term support (LTS) versions, enabling operating system vendors (OSVs) such as Kylinsoft, iSoft, Sinosoft, and GreatDB to develop commercial releases.



# Contents

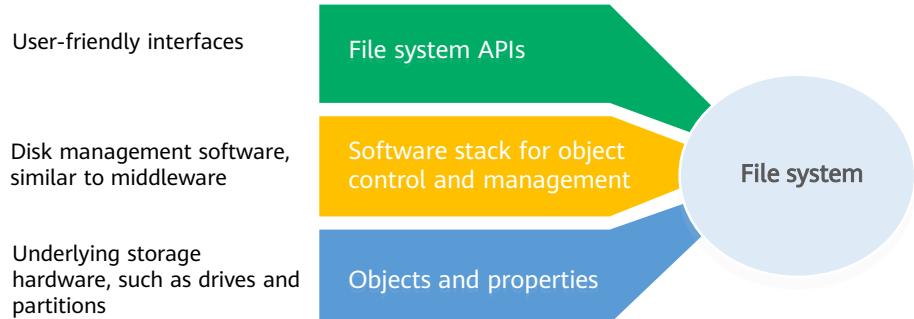
## 1. Operating System Basics

### 2. Linux Basics

- Introduction to Linux
- Introduction to openEuler
- **Introduction to File Systems on openEuler**
- Basic openEuler Operations

## File System Overview

- A file system is a method and a data structure used by an OS to identify files on a storage device or a partition, that is, a method of organizing files on a storage device.
- In an OS, a software structure that manages and stores file data is referred to as a file management system, or file system for short.



- Function: The file system organizes and allocates the space on file storage devices, stores files, and protects and retrieves the stored files. Specifically, it is responsible for creating files for users, saving, reading, modifying, and dumping files, controlling access to files, and canceling a file that is no longer in use. Functions of a file system include: manages and schedules storage space of a file, and provides the logical structure, physical structure, and storage method of the file; maps file identifiers to actual addresses, controls and accesses files, shares file information, provides reliable file confidentiality and protection measures, and provides file security measures.

## File Systems on openEuler

- The openEuler kernel is derived from Linux. The Linux kernel supports more than 10 types of file systems, such as Btrfs, JFS, ReiserFS, ext, ext2, ext3, ext4, ISO 9660, XFS, Minix, MSDOS, UMSDOS, VFAT, NTFS, HPFS, SMB, SysV and PROC. The following table describes the common file systems.
- The default file system on openEuler is ext4.

Common File System	Description
Ext	File system specially designed for Linux. The latest version is ext4.
XFS	A high-performance log file system developed for the IRIX OS by Silicon Graphics in 1993. Later ported to the Linux kernel, it excels in large-file processing and provides smooth data transfer.
VFAT	On Linux, VFAT is the name of the FAT (including FAT16 and FAT32) file systems in DOS and Windows.
ISO 9600	The standard file system for optical disc media. Linux supports this file system, allowing the system to read CD-ROMs and ISO image files, and burn CD-ROMs.

# Contents

## 1. Operating System Basics

### **2. Linux Basics**

- Introduction to Linux
- Introduction to openEuler
- Introduction to File Systems on openEuler
- Basic openEuler Operations

# Contents

## **Basic openEuler Operations**

- Basic Knowledge of Linux Commands
  - Basic openEuler Commands
  - Text Processing on openEuler
  - Network Management on openEuler

## Linux GUI and CLI

- A graphical user interface (GUI) presents all elements as graphical. The mouse is used as the main input tool, and buttons, menus, and dialog boxes are used for interaction, focusing on ease of use.
- All elements on a command line interface (CLI) are character-based. The keyboard is used as the input tool to enter commands, options, and parameters for executing programs, achieving high efficiency.

- Example:
  - Start the calculator on the Windows GUI. Choose **Start > Programs > Windows Accessories > Calculator**. In the calculator, click buttons to enter an expression. Similarly, a small keyboard is displayed when a certain program requires you to enter a password, asking you to click the numbers. This method is very user-friendly, and the calculator looks similar to the input device used at bank ATMs all around the world. The difference here is that you click it using a mouse, rather than using your own hands.
  - In the Linux CLI, enter **bc** to start the calculator. Enter the calculation **1 + 1** and press **Enter**. Result **2** is obtained.

## Why We Use CLIs

- Higher efficiency
  - On Linux, it is faster to perform operations on a keyboard than using the mouse.
  - A GUI-based operation cannot be repeated, while a CLI script can be used to complete all required tasks, for example, deleting outdated log files.
- Lower overheads compared with a GUI
  - Running a GUI requires a large amount of system resources. With the CLI, system resources can be released and allocated to other operations.
- Sometimes, the only choice
  - Most servers choose not to install a GUI.
  - Tools for maintaining and managing network devices do not provide a GUI.

## Linux CLI Shortcuts

- Tab completion
  - Use the **Tab** key to complete a command or file name, which is time-saving and accurate.
  - When no command is entered, press **Tab** twice to list all available commands.
  - If you have entered a part of the command name or file name, press **Tab** to complete it automatically.
- Cursor control
  - **↑**: Press **↑** several times to display historical commands for quick execution.
  - **↓**: Press **↓** together with **↑** for choosing a historical command.
  - **Home**: Press **Home** to move the cursor to the beginning of the line.
  - **Ctrl+A**: Press **Ctrl+A** to move the cursor to the beginning of the line.
  - **Ctrl+E**: Press **Ctrl+E** to move the cursor to the end of the line.
  - **Ctrl+L**: Press **Ctrl+L** to clear the screen.

## Login to Linux

- You can log in to Linux in either of the following ways:

- Local login

```
activate the web console with: systemctl enable --now cockpit.socket
openEuler login: root
Password: [REDACTED]
Last login: [REDACTED] from 192.168.56.1
Authorized users only. All activities may be monitored and reported.

Welcome to 4.19.90-2112.8.8.8131.on1.x86_64
System information as of time: [REDACTED]

System load: 0.62
Processes: 113
Memory used: 13.5%
Swap used: 0%
Usage On:
IP address: 192.168.56.10
IP address: 192.168.56.10
IP address: 192.168.122.1
Users online: 1

root@openEuler ~%#
```

- Remote Login

- Using clients such as PuTTY and Xshell to remotely log in to openEuler.

- After you log in to the system as the **root** user, **#** is displayed in the command prompt.

## Changing the Password

- Passwords are used to ensure the security of system and data.
- To ensure system security, you should:
  - Change the password upon the first login.
  - Change passwords periodically.
  - Set a complex password, for example, a password containing more than eight characters and at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters.
- You can run the **passwd** command to change the password.

```
[root@openEuler ~]# passwd
Changing password for user root.
New password:                                # Change the password of the current user.
Retype new password: # Enter the new password again.
passwd: all authentication tokens updated successfully
[root@openEuler ~]# passwd test1
Changing password for user test1.
New password:                                # Enter the new password.
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.          # Change the password of a common user as the root user.
```

- For security purposes, openEuler does not display the password when you enter it and does not use any placeholders to indicate the number of characters.

## Types of Linux Users

- On Linux, a UID is used to uniquely identify a user.
- Based on different UIDs, there are three types of users in Linux (openEuler is used as an example):
  - Super user
    - The super user is also called the super administrator. Its UID is 0. The super user has all system permissions. It is similar to the administrator in Windows.
  - System user
    - System users, also called program users, have UIDs ranging from 1 to 999. A system user is created by a program and is used to run the program or service.
  - Common user
    - Common users are generally created by the super administrator (the root user) to perform limited management and maintenance operations on the system. UIDs of common users range from 1000 to 60000.

## Creating and Deleting a Linux User

- Creating a user (common user by default): **useradd username**
- Viewing user information: **id username**
- Switching users: **su - username**
- Deleting a user: **userdel username**

```
[root@openEuler ~]# useradd user01          # Create user user01.  
[root@openEuler ~]# id user01                # View information about user01 as the root user.  
uid=1001(user01) gid=1001(user01) groups=1001(user01)  
[root@openEuler ~]# su - user01            # Switch to the user01 user. The command prompt changes to $.  
[user01@openEuler ~]$ id                  # Use the id command to view information about the current user  
by default.  
uid=1001(user01) gid=1001(user01) groups=1001(user01)  
[user01@openEuler ~]$ exit                # Log out of the current user.  
logout  
[root@openEuler ~]# userdel user01          # Delete user user01.
```

# Contents

## **Basic openEuler Operations**

- Basic Knowledge of Linux Commands
  - **Basic openEuler Commands**
  - Text Processing on openEuler
  - Network Management on openEuler

## Power Supply Commands: shutdown and reboot

- **shutdown** is used to shut down the computer, which requires root permissions.
  - Main options:
    - **-h**: powers off the computer after it is shut down.
    - **-r**: powers on the computer after it is shut down. (This operation is equivalent to restarting the computer.)
    - **-p**: explicitly indicates that the system will be shut down and the main power supply will be cut off.
- **reboot** is used to restart the computer, which requires system administrator permissions.
  - Main options:
    - **-w**: writes records to the **/var/log/wtmp** file. It does not restart the system.
    - **-d**: does not write records to the **/var/log/wtmp** file.
    - **-i**: restarts the system with network settings disabled.

- The **shutdown** command can safely shut down the system. It is dangerous to shut down the Linux system by directly powering off the system.
- Different from Windows, Linux runs many processes in the background. Therefore, forcible shutdown may cause loss of process data, making the system unstable and even damaging hardware in some systems.
- If you run the **shutdown** command to shut down the system, the system notifies all users who have logged in that the system will be shut down and the **login** command will be frozen, prohibiting new user logins.

## File Paths

- Absolute path: a path starting from the root directory (/), for example, /root/Desktop.
- Relative path: a path starting from the current path, for example, ./Desktop.
  - ./ or . indicates the current path. ../ or .. indicates the upper-level directory of the current path.
- **pwd:** Viewing the current path
- **cd:** Switching paths

```
[root@localhost ~]# pwd                                # View the current path.  
/root  
[root@localhost ~]# cd /root/Desktop                  # Go to the Desktop directory using the absolute path.  
[root@localhost Desktop]# cd                         # Run the cd command without a parameter to go to the home directory  
of the current user by default.  
[root@localhost ~]# cd ./Desktop                     # Go to the Desktop directory using a relative path.  
[root@localhost Desktop]# pwd                         # Switch to the home directory of the user. ~ indicates the home  
directory of the current user.  
[root@localhost ~]# pwd  
/root
```

- The **cd** command is used to change the current working directory.
- Syntax: **cd [directory]**
  - **cd /usr:** goes to the /usr directory.
  - **cd ..:** goes to the upper-level directory. Double dot indicates the upper-level directory.
  - **cd .:** goes to the current directory.
  - **cd:** goes to the home directory by default if no parameter is added.
  - **cd -:** goes to the previous directory. This command is used to quickly switch between two directories.
  - **cd ~:** goes to the home directory.

## Viewing Files

- **ls:** Viewing the content of a directory

```
[root@localhost ~]# ls -a          # List all files and directories.  
ifcfg-lo  ifdown-eth  ifdown-isdn  ifdown-routes  
[root@localhost ~]# ls -l          # Display detailed information about types, permissions,  
                                owners, and sizes of the files.  
total 228  
-rw-r---- 1 root root  86 Jun 15 19:03 ifcfg-eth0  
-rw-r---- 1 root root 254 Jun 15 19:03 ifcfg-lo
```

- **cat, tail, or head:** Viewing the content of a common file

```
[root@localhost ~]# cat ifcfg-eth0      # View all contents of the file.  
DEVICE="eth0"  
BOOTPROTO="dhcp"  
ONBOOT="yes"  
TYPE="Ethernet"  
PERSISTENT_DHCLIENT="yes"  
[root@localhost ~]# tail -2 ifcfg-eth0    # View the last two lines of the file.  
TYPE="Ethernet"  
PERSISTENT_DHCLIENT="yes"  
[root@localhost ~]# head -2 ifcfg-eth0     # View the first two lines of the file.  
DEVICE="eth0"  
BOOTPROTO="dhcp"
```

- The **ls** command is used to view contents of a directory.
  - **-a:** lists all files including hidden files.
  - **-l:** displays file details in long format.
  - **-R:** lists files in the subdirectories recursively.
  - **-t:** lists files by modification time.
- The **cat** command is used to view contents of a small file. This command displays all lines in a file.
- The **tail** command is used to view the last 10 lines of a file by default.
  - **-n:** followed by a number, for example, 5, indicating that the last five lines of a file are viewed. You can also enter a number directly without the **-n** option.
  - **-f:** dynamically displays file changes. This option is commonly used for viewing log files.
- The **head** command is used to view the first 10 lines of a file by default.
- The **less** and **more** commands are used to view large files page by page. Enter **q** to exit. Enter a slash (/) and a keyword to search for the keyword in the file.

## Creating Files

- **mkdir:** Creating directories (folders)

- -p: cascades to create multiple directories recursively.

```
[root@localhost ~]# mkdir my_dir_01          # Create a my_dir_01 directory.  
[root@localhost ~]# ls  
anaconda-ks.cfg  my_dir_01  
[root@localhost ~]# mkdir -p my_dir_02/sub_dir  # Create a my_dir_02 directory and its subdirectory sub_dir.
```

- **touch:** Creating common files

```
[root@localhost ~]# touch test01.log test02.log      # Create files test01.log and test02.log.  
[root@localhost ~]# ls -lt  
total 0  
-rw----- 1 root root 0 Jul 29 15:06 test01.log  
-rw----- 1 root root 0 Jul 29 15:06 test02.log
```

## Copying Files

- **cp:** Copying files or directories
  - **-a:** copies the files of a directory while retaining the links and file attributes.
  - **-r:** If the source file is a directory, all subdirectories and files in the directories are copied recursively and the attributes are retained.

```
[root@localhost ~]# ls
test01.log test02.log
[root@localhost ~]# cp /etc/passwd passwd.back          # Copy the /etc/passwd file to the current directory and rename the
file to passwd.back.

[root@localhost ~]# cp -r /var/log/audit .
[root@localhost ~]# ls
audit passwd.back test01.log test02.log
[root@localhost ~]# cp -s /etc/passwd passwd_link      # Create a symbolic link passwd_link of the passwd file.
[root@localhost ~]# ls -l
total 8
drwx----- 2 root root 4096 Jul 29 15:24 audit
-rw----- 1 root root 2546 Jul 29 15:24 passwd.back
lrwxrwxrwx 1 root root 11 Jul 29 15:25 passwd_link -> /etc/passwd
-rw----- 1 root root 0 Jan 2 19:20 test01.log
-rw----- 1 root root 0 Jul 29 19:20 test02.log
[root@localhost ~]#
```

- The **cp** command is used to copy files and directories. You can copy one or more files at a time. Exercise caution when running this command because data loss risks are involved.
- Syntax: **cp [OPTION]... SOURCE... DIRECTORY**
  - **-a:** copies the files of a directory while retaining the links and file attributes.
  - **-p:** copies the file content, modification time, and access permissions to the new file.
  - **-r:** if the source file is a directory, all subdirectories and files in the directories are copied recursively.
  - **-l:** creates a hard link of the source file instead of copying it.
  - **-s:** creates a soft link of the source file instead of copying it.
- **cp f1 f2:** copies file f1 and renames it to f2.
- **cp f1 d1/:** copies f1 to the d1 directory without renaming it.
- **cp f1 f2 f3 d1/:** copies multiple files to a directory.
- **cp -i f1 f2:** waits for the user's confirmation before overwriting f2 if f2 already exists.
- **cp -r d1 d2:** copies a directory recursively if the **-r** option is added.
- **cp -a f1 f2:** if the **-a** option is added, the attributes of the source file are retained. This option is used to copy block devices, character devices, and named pipes.
- By default, the **cp** command does not ask the user before overwriting files. Therefore, many shells have made **cp** as an alias for **cp -i**. The **-f** option in the **cp** command does not indicate forcible overwriting.

## Moving and Renaming Files

- **mv:** Moving or renaming a file
  - The **mv** command is used to move a file or directory. Exercise caution when running this command because data loss risks are involved.
  - If the source file and target file are in the same directory, the **mv** command is used to rename the file.

```
[root@localhost ~]# ls  
passwd_link test01.log test02.log  
[root@localhost ~]# mv test02.log test03.log      #Change the name of the test02.log file to test03.log  
[root@localhost ~]# ls  
passwd_link test01.log test03.log  
[root@localhost ~]# mv test01.log /root/test      # Move the test01.log file to the /root/test directory.  
[root@localhost ~]# mv -f test01.log test03.log    # Forcibly overwrite the test03.log file with the content of  
                                                the test01.log file.
```

- The **mv** command is used to move a file or directory. Exercise caution when running this command because data loss risks are involved.
- If the source file and target file are in the same directory, the **mv** command renames the file.
- Syntax: **mv [option] source\_file\_or\_directory target\_file\_or\_directory**
  - **-b:** backs up a file before overwriting it.
  - **-f:** forcibly overwrites the target file without asking the user.
  - **-i:** overwrites the target file after obtaining the user's consent.
  - **-u:** updates the target file only when the source file is newer than the target.

# Deleting Files

- **rm:** Deleting files or directories
  - The **rm** command is a high-risk command. No tool can guarantee recovery of files deleted by the **rm** command, which does not move a file to a recycle bin like in GUIs. Therefore, you cannot undo the deletion.

```
[root@localhost ~]# ls  
audit_back passwd.back test01.log test03.log  
[root@localhost ~]# rm test01.log  
  
rm: remove regular empty file 'test01.log'? yes  
[root@localhost ~]# rm -rf test03.log  
[root@localhost ~]# rm -rf audit_back/  
  
[root@localhost ~]# ls  
passwd.back  
[root@localhost ~]#
```

# Delete the test01.log file with a prompt before deletion.

# Forcibly delete the test03.log file.

# Delete the mail.bak directory, including all files and subdirectories in it.

- Syntax: **rm [OPTION] file\_or\_directory**
  - **-f, --force:** ignores the files that do not exist and does not display any message.
  - **-i, --interactive:** performs interactive deletion.
  - **-r, -R, --recursive:** recursively deletes all directories listed as arguments and their subdirectories.
  - **-v, --verbose:** displays the detailed progress.

## Obtaining Help Information About a Command

- **help:** Obtaining simple help information about a command
  - To navigate the massive number of commands on Linux, you can run the **help** command to obtain help information.
  - Syntax: **[command] --help** or **help [command]**.

```
[root@localhost ~]# help pwd
pwd: pwd [-LP]
    Print the name of the current working directory.
  Options:
    -L      print the value of $PWD if it names the current working directory
    -P      print the physical directory, without any symbolic links

  By default, 'pwd' behaves as if '-L' were specified.

  Exit Status:
    Returns 0 unless an invalid option is given or the current directory cannot be read.
[root@localhost ~]# systemctl --help
systemctl [OPTIONS...] {COMMAND} ...

  Query or send control commands to the systemd manager.

  -h --help      Show this help
  --version     Show package version
  --system      Connect to system manager
  -H --host=[USER@]HOST.....
```

38      Huawei Confidential



- The Linux system has so many commands that it is impossible to remember them all. However, you can run the **help** command to obtain help information.
- Syntax:
  - **help [option] [command]**
- The options are as follows:
  - **-d:** displays a brief description of the command topic.
  - **-s:** displays a brief description of the command syntax.

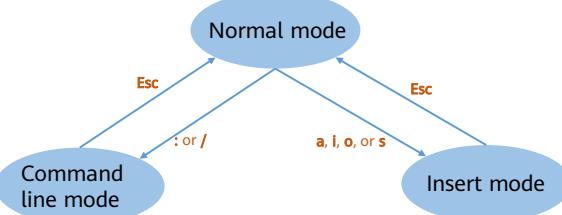
# Contents

## **Basic openEuler Operations**

- Basic Knowledge of Linux Commands
- Basic openEuler Commands
- **Text Processing on openEuler**
- Network Management on openEuler

## Linux Text Editor - Vim

- Vim is a customizable text editor derived from Visual Editor (vi) that inherits, improves and adds many features to vi's original base.
- Common Vim modes:
  - Normal mode: used to copy, paste, and delete text, undo previous operations, and navigate the cursor.
  - Insert mode: used to edit and modify text.
  - Command line mode: used to save, exit, search for, or replace text. Enter a colon (:) to switch to this mode.



- Vim is not installed on openEuler 20.03 LTS by default. You need to manually install it.

## Normal Mode of Vim

- By default, Vim begins to run in normal mode after you open a file with the **vim** command.

vim [options] [file]...	Edit specified files.
vim [options] -	Read text from standard input (stdin).
vim [options] -t tag	Edit the file where the tag is defined.
vim [options] -q [errorfile]	Edit the file where the first error occurs.

- Common options:

- **-c**: runs a specified command before opening a file.
- **-R**: opens a file in read-only mode but allows you to forcibly save the file.
- **-M**: opens a file in read-only mode and does not allow you to forcibly save the file.
- **-r**: recovers a crashed session.
- **+num**: starts at line *num*.

# Common Operations in Vim Normal Mode

- Cursor control
  - Arrow keys or **k**, **j**, **h**, and **l** keys move the cursor up, down, left, and right, respectively.
  - **0**: moves the cursor to the beginning of the current line.
  - **g0**: moves the cursor to the leftmost character of the current line that is on the screen.
  - **:n**: moves the cursor to line *n*.
  - **gg**: moves the cursor to the first line of the file.
  - **G**: moves the cursor to the last line of the file.
- Data operations
  - **yy** or **Y**: copies an entire line of text.
  - **y/nw**: copies 1 or *n* words.
  - **d/nw**: deletes (cuts) 1 or *n* words.
  - **/n/d**: deletes (cuts) 1 or *n* lines.

## Insert Mode of Vim

- Use the **vim** *filename* command to open a file and enter the normal mode by default. Type **i**, **I**, **a**, **A**, **o**, or **O** to enter the insert mode.
- If the *filename* file exists, the file is opened and the file content is displayed; otherwise, Vim displays **[New File]** at the bottom of the screen and creates the file when saving the file for the first time.
- Press **Esc** to exit the insert mode and return to the normal mode.

```
[root@openEuler ~]# vim test.txt          # Enter the normal mode by default.  
~  
~  
"test.txt" [New File]  
[root@openEuler ~]# vim test.txt          # Press i, I, a, A, o, or O to enter the insert mode.  
~  
~  
-- INSERT --
```

# Command Line Mode of Vim

- Search
  - `:/word or /word`: searches for a `word` string after the cursor. Press **n** to continue to search forwards or press **Shift+n** to search backwards.
- Replace
  - `:1,5s/word1/word2/g`: replaces all occurrences of `word1` in lines 1 to 5 with `word2`. If **g** is not specified, only the first occurrence of `word1` in each line is replaced.
  - `%s/word1/word2/gi`: replaces all occurrences of `word1` with `word2`. **i** ignores the case of matches.
- Save and exit
  - `:w`: Save the file and do not exit.
  - `:wq`: Save the file and exit.
  - `:q`: Exit without saving the file.
  - `:q!`: Exit forcibly without saving changes to the file.
  - `:wq!`: Forcibly save the file and exit.

# Contents

## **Basic openEuler Operations**

- Basic Knowledge of Linux Commands
- Basic openEuler Commands
- Text Processing on openEuler
- Network Management on openEuler

## Important Network Concepts in openEuler

- **Host network device:** a network adapter on the host.
- **Interface**
  - Interfaces on devices are created by drivers for the system access.
- **Broadcast address**
  - An IP address used to send packets to all hosts on the network segment
- **Subnet mask**
  - A number that distinguishes the network address and the host address within an IP address
- **Route**
  - Next-hop IP address when IP packets are transmitted across network segments
- **Link:** connection between the device and the network.



## Commands for Querying IP Addresses

- **ip** and **ifconfig** commands are used to view IP addresses of the current host.
- Viewing information about all network adapters on a host.

```
[root@openEuler ~]# ifconfig -a  
[root@openEuler ~]# ip addr show
```

- Viewing information about a specified interface on a host.

```
[root@openEuler ~]# ifconfig enp0s3  
[root@openEuler ~]# ip addr show enp0s3
```

- Viewing the current IP addresses and subnet masks of all interfaces: **ip addr**

## Configuring Static IP Addresses Using Network Adapter Configuration Files

- Query the path of the network adapter configuration file:

```
[root@openEuler ~]# ls /etc/sysconfig/network-scripts/ifcfg-*
/etc/sysconfig/network-scripts/ifcfg-enp0s3  /etc/sysconfig/network-scripts/ifcfg-enp0s8
```

- Parameter description:

Parameter	Description
TYPE	Interface type
BOOTPROTO	Boot-time protocol
ONBOOT	Whether to activate the device at boot-time
IPADDR	IP address
NETMASK	Subnet mask
GATEWAY	Gateway address
BROADCAST	Broadcast address
HWADDR/MACADDR	MAC address. Only one MAC address needs to be set. New MAC addresses cannot share the same name as another when they are set at the same time.
PEERDNS	Whether to specify the DNS server address. If the DHCP protocol is used, the default value is yes.
DNS{1, 2}	DNS server addresses
USERCTL	User permission control
NAME	Network connection name
DEVICE	Physical interface name

## Configuring the IP Address - Configuration File Example

- Set the static IP address of the enp0s3 interface to **192.168.56.100/24**.

```
TYPE=Ethernet
BOOTPROTO=static
NAME=enp0s3
DEVICE=enp0s3
ONBOOT=yes
IPADDR=192.168.56.100
NETMASK=255.255.255.0
```

- Restart the network.

```
[root@openEuler ~]# nmcli connection reload enp0s3
[root@openEuler ~]# nmcli connection up enp0s3
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/12)
```

- Sometimes, too many configuration items increase the difficulty of network troubleshooting.

# Configuring the Static IP Address Using the nmcli Command

- Check network connections of the current host.

```
[root@openEuler ~]# nmcli connection show
NAME      UUID                                  TYPE      DEVICE
enp0s3   3c36b8c2-334b-57c7-91b6-4401f3489c69  ethernet  enp0s3
enp0s8   00cb8299-feb9-55b6-a378-3fdc720e0bc6  ethernet  enp0s8
```

- Configure a static IP address.

```
[root@openEuler ~]# nmcli connection modify enp0s3 ipv4.method manual ipv4.addresses "10.0.2.10/24" ipv4.gateway "10.0.2.2"
```

- Restart the network.

```
[root@openEuler network-scripts]# nmcli connection reload enp0s3
[root@openEuler network-scripts]# nmcli connection up enp0s3
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/18)
```

- View the IP address.

```
[root@openEuler ~]# ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7d:e1:a5 brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.10/24 brd 10.0.2.255 scope global noprefixroute enp0s3
            valid_lft forever preferred_lft forever
```

- **conn**: indicates that an operation is to be performed on a connection.
- **add**: adds (a connection)
- **type**: type of the connection
- **con-name**: connection name
- **<ifname>**: name of the network adapter
- **mod**: modifies (a connection)

## Introduction to Routes

- To facilitate communication between two hosts in different subnets, a mechanism is required to describe the path for traffic. This mechanism is called routing, which is set using routing entries.
- A routing entry is a pair of predefined addresses, including the destination and gateway. It indicates a gateway through which the destination can be reached.
- The routing table is a collection of routing entries.

- Detailed description of routes:  
<https://docs.freebsd.org/en/books/handbook/advanced-networking/#network-routing>

## Route Management and Configuration

- In openEuler, the **route** command is used to view, configure, and manage local routes.
- In addition to the **route** command, the **ip** command can also be used to manage system routes.
- These commands will modify the routing table of the system. When the system is started, the routing table is loaded to the memory and maintained by the kernel.

- The **route**, **ip**, and **nmcli** commands can be used to manage routes. The following uses the **route** command as an example.

## Viewing the Routing Table Using the route Command

- Run the **route** command to view the routing table.

```
[root@openEuler ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         192.168.110.254 0.0.0.0      UG    100    0      0 enp4s0
192.168.110.0   0.0.0.0        255.255.255.0 U     100    0      0 enp4s0
192.168.122.0   0.0.0.0        255.255.255.0 U     0      0      0 virbr0
```

- When the **-n** option is used to display routes, the values in the **Destination** column are IP addresses.
- Eight fields are displayed when you run the route command to view routes. The possible values of the **Flags** field include:
  - U** (up) indicates that the route is up.
  - H** (host) indicates that the gateway is a host.
  - G** (gateway) indicates that the gateway is a router.
  - R** (reinstate) indicates that the route is reinstated for dynamic routing.
  - D** (dynamically) indicates that the route is dynamically written.
  - M** (modified) indicates that the route is dynamically modified by the routing daemon or redirect.
  - !** indicates that the route is closed.

## Adding a Route Using the route Command

- Add a (temporary) route to a network segment or host.

```
route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]] [if Interface]
```

- Example:

```
[root@openEuler ~]# route add -net 192.168.101.0 netmask 255.255.255.0 dev enp4s0
[root@openEuler ~]# route add -host 192.168.101.100 dev enp4s0
[root@openEuler ~]# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags   Metric   Ref  Use     Iface
default         _gateway       0.0.0.0       UG        100      0    0          enp4s0
192.168.100.10 0.0.0.0       255.255.255.255  UH        0        0    0          enp4s0
192.168.101.0  0.0.0.0       255.255.255.0    U        0        0    0          enp4s0
192.168.110.0  0.0.0.0       255.255.255.0    U        100      0    0          enp4s0
192.168.122.0  0.0.0.0       255.255.255.0    U        0        0    0          virbr0
```

- You can use the **route** command to add routes. The added routes are stored in the memory and become invalid after the system is restarted.
- The **route add -net 192.168.101.0 netmask 255.255.255.0 dev enp3s0** command adds a route to the 192.168.101.0/24 segment through the enp3s0 device.
- The **route add -host 192.168.101.100 dev enp3s0** command adds a route to the 192.168.101.100 host through the enp3s0 device.
- The output of the **route** command shows that routes to hosts have a higher priority than routes to network segments.

## Deleting a Route Using the route Command

- Deleting a route to a network segment or host using the **route del** command.

- Syntax:

```
route del [-net|-host] [netmask Nm] [gw Gw] [[dev] If]
```

- Example:

```
[root@openEuler ~]# route del -host 192.168.100.10 dev enp4s0
[root@openEuler ~]# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
default         _gateway       0.0.0.0        UG    100   0      0 enp4s0
192.168.101.0  0.0.0.0        255.255.255.0  U     0      0      0 enp4s0
192.168.110.0  0.0.0.0        255.255.255.0  U     100   0      0 enp4s0
192.168.122.0  0.0.0.0        255.255.255.0  U     0      0      0 virbr0
```

- The **route del -net 192.168.101.0 netmask 255.255.255.0 dev enp3s0** command deletes the route to the 192.168.101.0/24 segment. To delete a route to a network segment, the network segment and subnet mask parameters are mandatory, while the device parameter is optional.
- The **route del -host 192.168.101.100 dev enp3s0** command deletes the route to the 192.168.101.100 host. The device parameter is optional.
- To delete routes in the **route** file, use the vi editor to edit the file and restart the network.

## Host Name

- A host name identifies a device in a local area network (LAN).
- The device can be a physical or virtual machine.
- The host name is stored in the **/etc/hostname** file.

```
[root@openEuler ~]# cat /etc/hostname  
openEuler
```

## Setting the Host Name

- Setting a temporary host name: **hostname new-name**
- Setting a permanent host name: **hostnamectl set-hostname new-name**
- Setting a host name by modifying the file: write **new-name** to the **/etc/hostname** file.

```
[root@openEuler ~]# hostname  
openEuler  
[root@openEuler ~]# hostname huawei  
[root@openEuler ~]# hostname  
huawei  
[root@openEuler ~]# hostnamectl set-hostname openEuler01  
[root@openEuler ~]# hostname  
openEuler01  
[root@openEuler ~]# echo "HCIA-openEuler" > /etc/hostname
```

- To make the setting take effect, log in again or run the **source .bashrc** command.
- Run the **hostname** command to view the host name of the current system.

## Introduction to the hosts File

- Hosts in a LAN can be accessed through IP addresses.
- IP addresses are difficult to remember when a large number of hosts exist in the LAN. Therefore, we want to access the hosts directly through their host names.
- In this case, the hosts can be located using a table that records the mapping between host names and IP addresses. This table is the **hosts** file.

```
[root@openEuler ~]# cat /etc/hosts
127.0.0.1    localhost    localhost.localdomain    localhost4    localhost4.localdomain4
::1          localhost    localhost.localdomain    localhost6    localhost4.localdomain6
```

- The **hosts** file is a system file without a file name extension. Its basic function is to establish a "database" of frequently used domain names and their corresponding IP addresses.
- When a user enters a website URL in the web browser, the system searches for the corresponding IP address in the **hosts** file. Once the IP address is found, the system opens the corresponding web page.
- If the URL is not found, the system sends the URL to the DNS server for IP address resolution.
- Run the **cat /etc/hosts** command to view the **hosts** file.

## Modifying the hosts File

- You can edit the **hosts** file in the following format:

```
# Ip domain.com  
192.168.10.20 www.example.com
```

- To delete an entry, add **#** to comment it out. For example:

```
#ip domain.com  
#192.168.10.20 www.example.com
```

# Quiz

1. Which of the following statements is incorrect about file systems?
  - A. A file system is a method and a data structure used by an OS to identify files on a storage device or a partition.
  - B. The software structure that manages and stores file data is referred to as a file management system.
  - C. The file system manages and controls computer hardware and software resources.
  - D. The file system organizes and allocates the space on file storage devices, stores files, and protects and retrieves the stored files.
2. Linux is a multi-user OS that allows multiple users to log in at the same time and allows one user to log in multiple times.
  - A. True
  - B. False

- Answer:

- C
  - A

## Summary

- This course discusses the basic components and types of OSs and basic operations of Linux. Now, we have finished learning the basics about computing, storage, network, and OS technologies. In cloud computing, how can we use and manage the resources to provide services for applications? We will address these issues in the next course about virtualization technology.

# 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

CLI: Command Line Interface

GUI: Graphical User Interface

POSIX: Portable Operating System 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.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



# 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

- Upon 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.

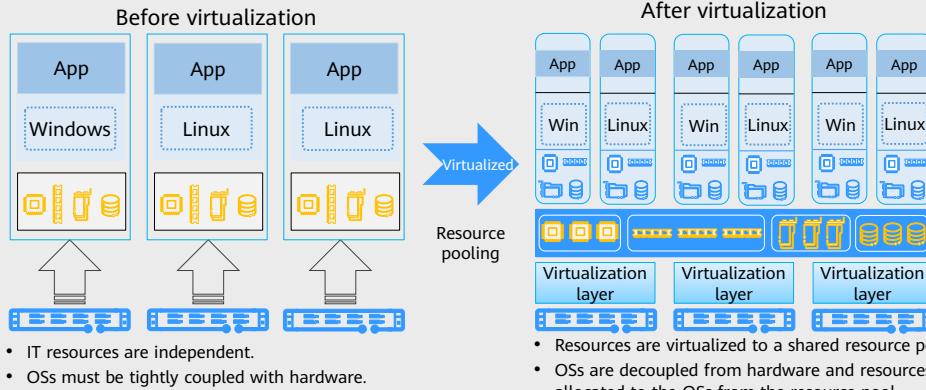
# Contents

## **Overview**

- Virtualization
- Mainstream Virtualization Technologies

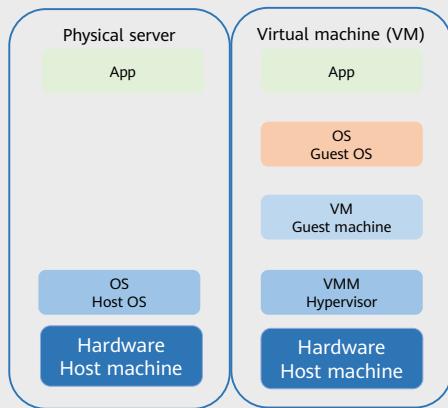
## What Is Virtualization?

- 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).



- 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)

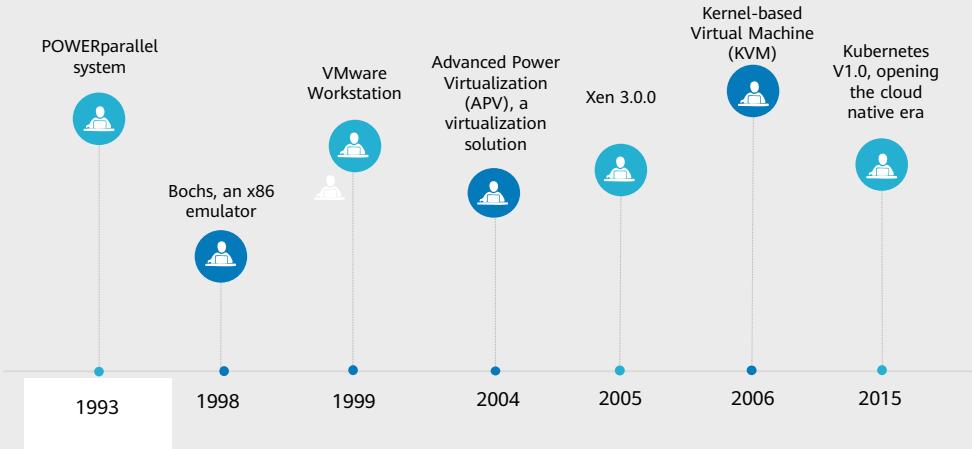
## Host OS

OS running on a physical machine (PM)

## Host Machine

PM

## Virtualization History

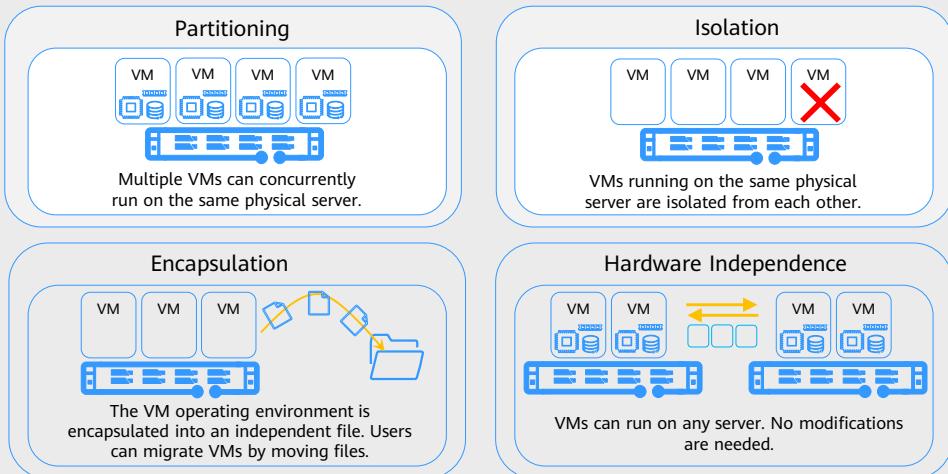


- In 1993, IBM launched an upgradeable POWERparallel system, the first microprocessor-based supercomputer using RS/6000 technology.
- In 1998, Bochs, an x86 emulator, was released.
- In 1998, VMware was founded. In 1999, the company launched VMware Workstation, the commercial virtualization software, that can run smoothly. Since then, virtualization has been widely applied.
- In 1999, IBM first proposed the logical partitions (LPARs) for the AS/400 system.
- In 2000, Citrix released XenDesktop, a desktop virtualization product.
- In 2004, IBM released the virtualization solution Advanced Power Virtualization (APV), which supports resource sharing. This solution was renamed PowerVM in 2008.
- In 2005, Xen 3.0.0 was released as the first hypervisor that supports Intel® Virtualization Technology-x (Intel® VT-x). It can run on 32-bit servers.
- In 2006, Qumranet, an Israeli startup, officially announced Kernel-based Virtual Machine (KVM).
- 2006–present: cloud computing and big data era
- In 2007, InnoTek, a German company, developed VirtualBox.
- In 2008, Linux Container (LXC) 0.1.0 was released to provide lightweight virtualization.
- In 2010, Red Hat released RHEL 6.0, removing Xen virtualization installed by default and providing KVM virtualization.
- In 2015, Kubernetes v1.0 was released, opening the cloud native era.

## 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.

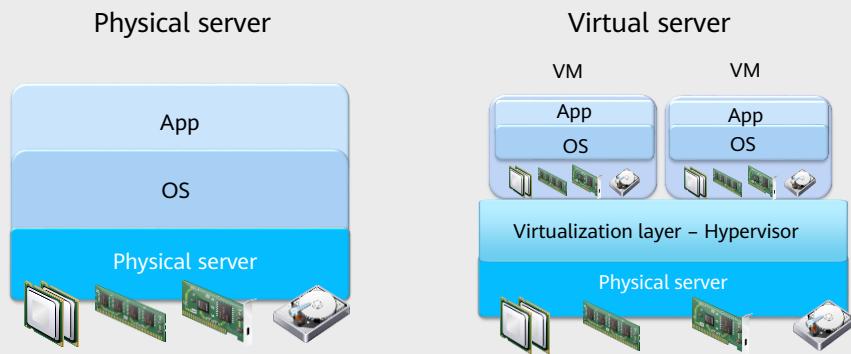
## Virtualization Characteristics



- **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.

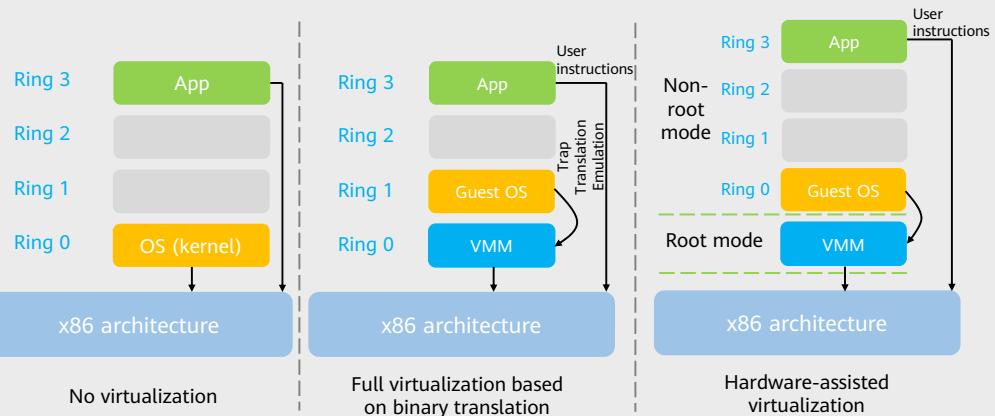
## Advantages of Virtualization



- 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.

- 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.

## CPU Virtualization

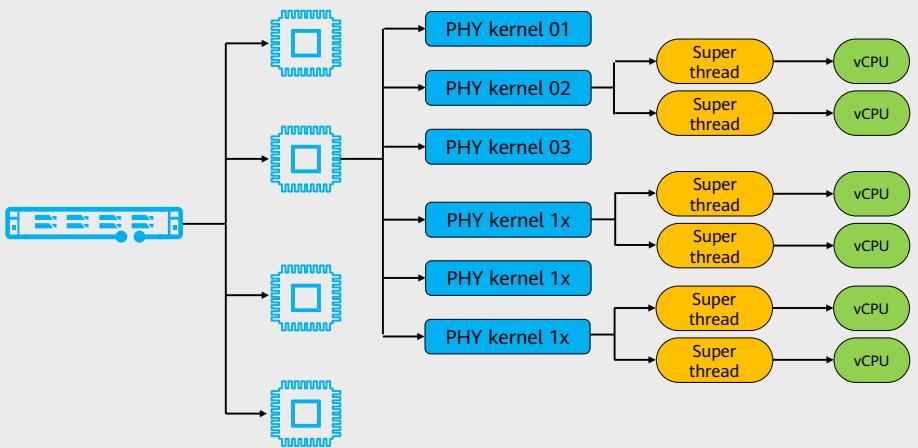


- x86 OSs run directly on bare hardware devices, so they naturally assume they fully "own" the computer hardware. The x86 architecture provides four privilege levels for OSs and apps to access hardware. Ring indicates the protection ring in an OS. Rings are arranged in a hierarchy from the most privileged (the most trusted, usually numbered zero) to the least privileged (the least trusted, usually with the highest ring number): Ring 0, Ring 1, Ring 2, and Ring 3. For the x86-based Linux:
  - Since the OS (kernel) needs to directly access hardware and memory, its code needs to run in Ring 0. In this way, the OS can use privileged instructions to control interrupts, modify page tables, and access devices.
  - The app code running in Ring 3 cannot perform control operations. If you want to access a disk or write a file, you need to execute a system call (function). When the system call is executed, the protection ring is switched from Ring 3 to Ring 0, and jumps to the corresponding kernel code. In this way, the device is accessed by the kernel and then the protection ring returns to Ring 3 from Ring 0. This process is also called switching between the user mode and kernel mode.
- Virtualization encounters a problem. The host OS works in Ring 0, so the guest OS cannot work in Ring 0. However, the guest OS does not know this rule and still executes what instructions were executed in the past. If the guest OS does not have the execution permission, an error will occur. VMM is required to avoid this error. The VM uses the VMM to enable the guest CPU to access the hardware. There are three technologies based on different principles:
  - Full virtualization
  - Paravirtualization

- Hardware-assisted virtualization
- After 2005, CPU vendors Intel and AMD began to support virtualization. Intel introduces the Intel-VT technology. This type of CPU with Intel-VT technology has two modes: VMX root operation and VMX non-root operation. Both modes support four protection rings of Ring 0 to Ring 3. This enables the VMM to run in VMX root operation mode, and the guest OS to run in VMX non-root operation mode.

- Hardware-assisted virtualization for processors includes Intel VT-x and AMD-V. New instructions and running modes are introduced to allow the VMM to run in root mode and the guest OSs running in Ring 0 to run in non-root mode. Generally, core instructions from the guest OS can reach and be executed on the hardware without being transferred to the VMM. When the guest OS receives special instructions, the system transfers the instructions to the VMM for processing.
- For example, the Intel VT technology adds two running modes: VMX root mode and VMX non-root mode. Generally, the host OS and VMM run in VMX root mode, and the guest OS and its applications run in VMX non-root mode. Both modes support all rings. The guest machine can run in the required ring (the OS runs in Ring 0, and the applications run in Ring 3). The VMM also runs in the required ring. QEMU runs in Ring 3, and KVM runs in Ring 0. The switching of the CPU between the two modes is called VMX switching. Entering the non-root mode from the root mode is VM-Entry. Entering the root mode from the non-root mode is VM-Exit. CPUs are controlled to switch between the two modes, and execute VMM code and guest OS code in turn.
- For the KVM, the VMM running in VMX root mode executes the VMLAUNCH instruction to switch the CPU to VMX non-root mode when executing the guest OS instructions, and starts to execute the guest code. This process is VM-Entry. When the guest OS needs to exit this mode, the CPU is automatically switched to the VMX root mode. The process is VM-Exit. Obviously, the KVM guest code is controlled by the VMM and runs directly on the CPU. QEMU controls the VM code to be executed by the CPU through KVM, but it does not execute the VM code.

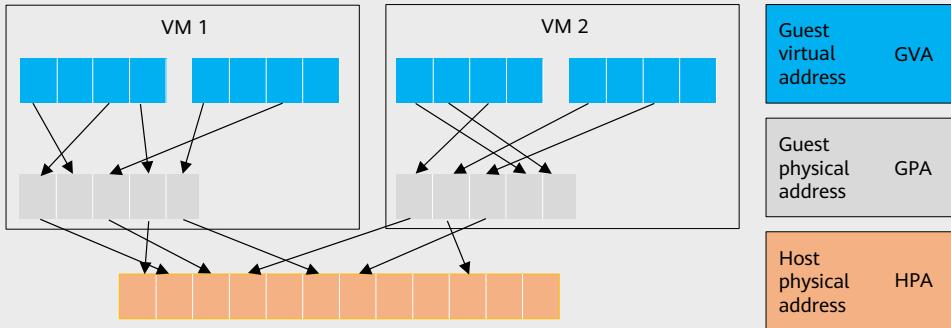
## Mappings Between CPUs and vCPUs



- 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 ( $2 \times 8 \times 2$ ). The total CPU frequency is calculated as follows:  $32 \times 2.6 \text{ GHz} = 83.2 \text{ GHz}$ .
- 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

- 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.



14      Huawei Confidential



- 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).

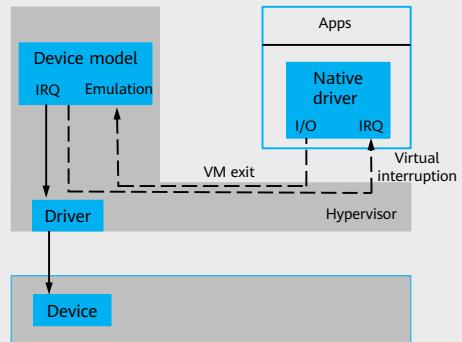
## I/O Virtualization

- 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 needs to solve the following problems:
  - Device discovery
    - Control over devices that VMs can access
  - Access interception
    - Access to devices through I/O ports or memory-mapped I/O (MMIO)
    - Data exchanges between a device and memory through direct memory access (DMA)

## 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

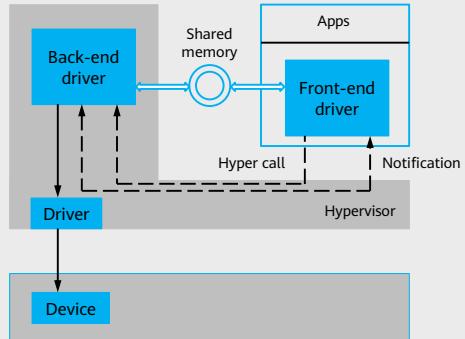
- Disadvantages of I/O virtualization

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

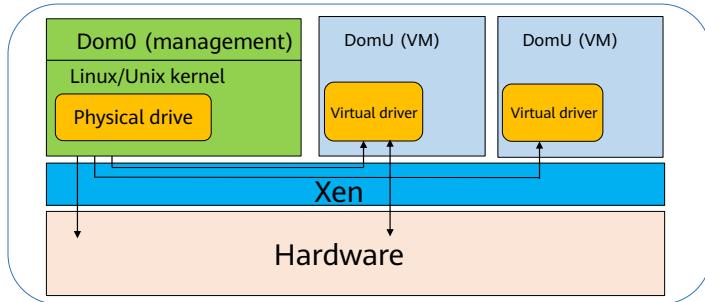
# Contents

## 1. Overview

- Virtualization
- Mainstream Virtualization Technologies

## 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.



19      Huawei Confidential



- 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](http://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

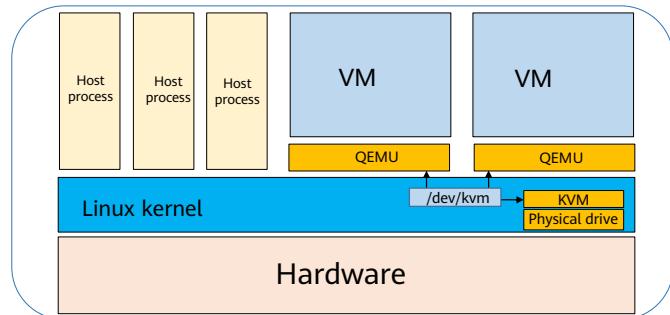
- KVM is a kernel-based VM.
- The essence of KVM is kvm.ko, a virtualization module in the Linux kernel. It uses Linux to perform operations, such as task scheduling, memory management, and interaction with hardware devices.
- KVM is open-source software that was integrated into the Linux 2.6.20 kernel 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 vendors 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.

## 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.



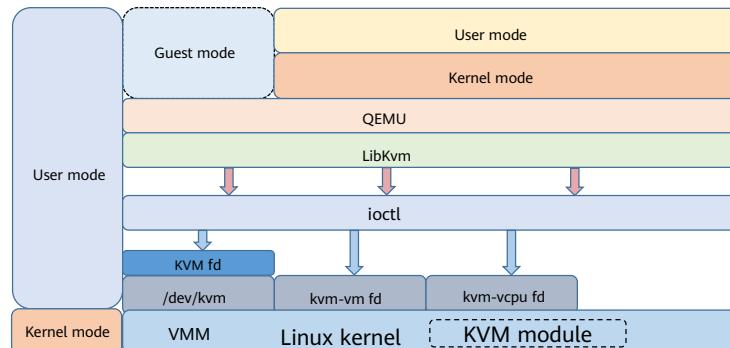
21 Huawei Confidential



- 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.

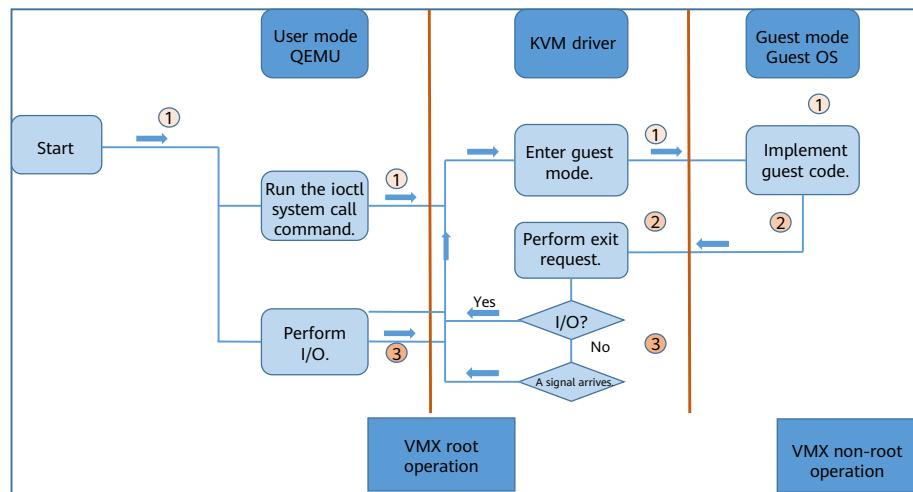
# Working Principles of KVM

- 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.

## (Optional) Working Principles of KVM



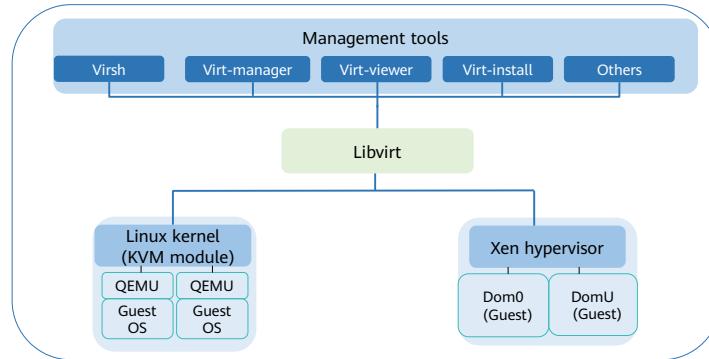
23      Huawei Confidential



- 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.

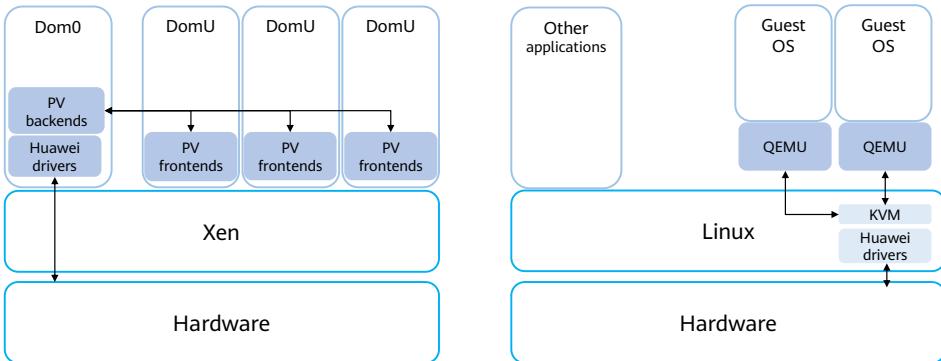


24 Huawei Confidential



- 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.

## Xen vs. KVM



- 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.

# 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.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



# Huawei Virtualization Platform



# Foreword

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

# Objectives

Upon completion of this course, you will understand:

- Basic components of the FusionCompute virtualization suite.
- Architecture, positioning, and features of FusionCompute.
- Functions of FusionCompute.
- Planning and deployment of FusionCompute.

# Contents

- 1. Introduction to FusionCompute**
  - FusionCompute Virtualization Suite
    - FusionCompute Positioning and Architecture
    - FusionCompute Functions
2. FusionCompute Planning and Deployment

## FusionCompute Virtualization Suite

- Huawei FusionCompute virtualization suite is a leading virtualization solution that improves infrastructure efficiency for data centers. It provides the following benefits:
  - Better infrastructure utilization
  - Significantly faster service rollout
  - Much lower power consumption
  - Rapid automatic fault recovery based on high availability and powerful restoration features, lowering data center cost and increasing system uptime
- This suite virtualizes hardware resources using the virtualization software deployed on physical servers, so that one physical server serves as multiple virtual servers. It consolidates existing workloads and uses available servers to deploy new applications and solutions, realizing a high integration rate.

- Application scenario:
  - Single-hypervisor applies if 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 compute, virtual storage, and virtual network technologies. It centrally schedules and manages virtual resources over unified interfaces, thereby ensuring high system security and reliability and reducing the OPEX.

# Contents

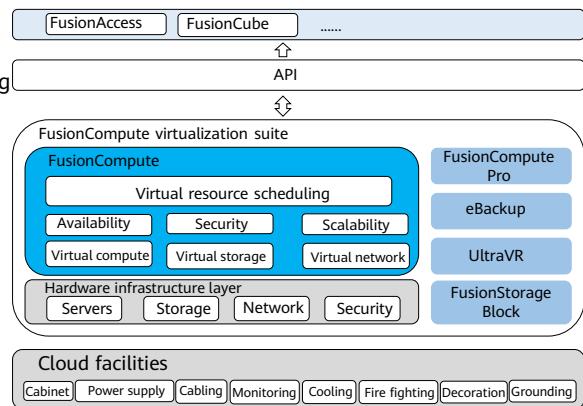
- 1. Introduction to FusionCompute**
  - FusionCompute Virtualization Suite
    - FusionCompute Positioning and Architecture
    - FusionCompute Functions
2. FusionCompute Planning and Deployment

## FusionCompute Positioning

- FusionCompute is a cloud OS software that virtualizes hardware resources and centrally manages virtual, service, and user resources. It virtualizes compute, storage, and network resources using the virtual compute, storage, and network technologies.
- By centrally scheduling and managing virtual resources on unified interfaces, FusionCompute provides high system security and reliability while reducing OPEX. It helps carriers and other enterprises build secure, green, and energy-saving cloud data centers.

# Position of FusionCompute in the Virtualization Suite

- Cloud facilities
- Hardware infrastructure
  - Basic physical devices of cloud computing
  - FusionStorage Block
- FusionCompute virtualization suite
  - FusionCompute
  - FusionCompute Pro
  - eBackup
  - UltraVR

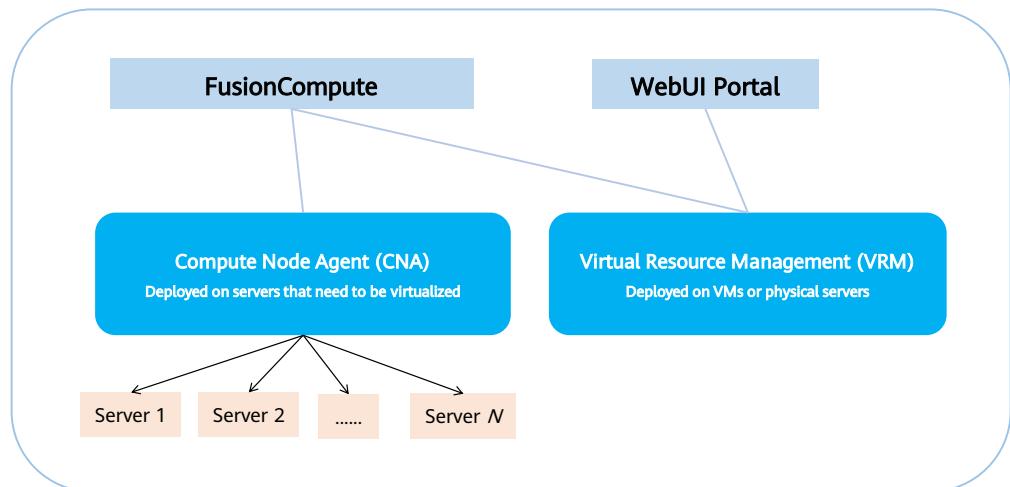


- Cloud facilities refer to the auxiliaries and space required by the cloud data center, including the power system, fire-fighting system, wiring system, and cooling system.
- Hardware infrastructure layer:
  - Hardware infrastructure consists of servers, storage devices, network devices, and security devices. These resources allow customers to build different scales of 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 (FusionStorage Block) is a distributed storage software that provides both storage and compute capabilities. It can be deployed on general-purpose servers to consolidate the local disks of all the servers into a virtual storage resource pool to provide the block storage function.
- 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. It maximizes resource utilization by consolidating existing workloads on some servers and therefore releasing more servers to carry new applications and solutions.
  - FusionCompute is a cloud OS software that virtualizes hardware resources and centrally manages virtual, service, and user resources. It virtualizes compute, storage, and network resources using the virtual compute, storage, and network technologies. By centrally scheduling and managing virtual resources on unified interfaces, FusionCompute provides high system security and reliability while reducing OPEX. It helps carriers and other

enterprises build secure, green, and energy-saving cloud data centers.

- 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, which provides data protection and DR for key VM data using the asynchronous remote replication feature provided by the underlying SAN storage system.
- FusionCompute Pro is a component for unified management of multiple resource sites in different regions. It uses virtual data centers (VDCs) to provide domain-based resource management capabilities for different users.

## FusionCompute Architecture



- 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	Deployed on servers that need to be virtualized.	<ul style="list-style-type: none"><li>• Implementing the virtual computing function</li><li>• Managing the VMs running on compute nodes</li><li>• Managing compute, storage, and network resources on compute nodes</li></ul>
VRM	Deployed on VMs or physical servers. VRM provides a web interface for management and maintenance personnel.	<ul style="list-style-type: none"><li>• Managing block storage resources in a cluster</li><li>• Managing network resources, such as IP addresses and virtual local area network (VLAN) IDs, in a cluster and allocating IP addresses to VMs</li><li>• Managing the life cycle of VMs in a cluster and distributing and migrating VMs across compute nodes</li><li>• Dynamically adjusting resources in a cluster</li><li>• Implementing centralized management of virtual resources and user data and providing elastic computing, storage, and IP address services</li><li>• Allowing O&amp;M engineers to remotely access FusionCompute through one unified web interface to perform resource monitoring and management and view resource statistics reports</li></ul>

11      Huawei Confidential



- CNA provides the following functions:
  - Implementing the virtual computing function
  - Managing the VMs running on compute nodes
  - Managing compute, storage, and network resources on compute nodes
- VRM provides the following functions:
  - 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 life cycle 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

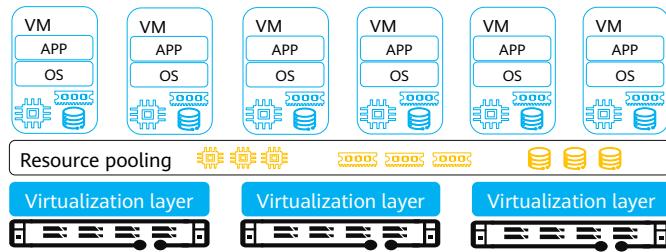
## **1. Introduction to FusionCompute**

- FusionCompute Virtualization Suite
- FusionCompute Positioning and Architecture
- **FusionCompute Functions**

## **2. FusionCompute Planning and Deployment**

## FusionCompute Functions - Virtual Computing

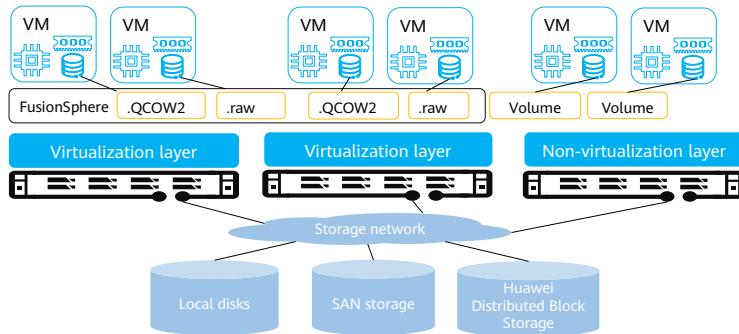
- FusionCompute enables physical server resources to be converted to logical resources. It divides a server into multiple isolated virtual compute resources, while CPU, memory, disk, and I/O resources become pooled resources that are dynamically managed. This increases the resource utilization and simplifies system management.
- 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 Functions - Virtual 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.



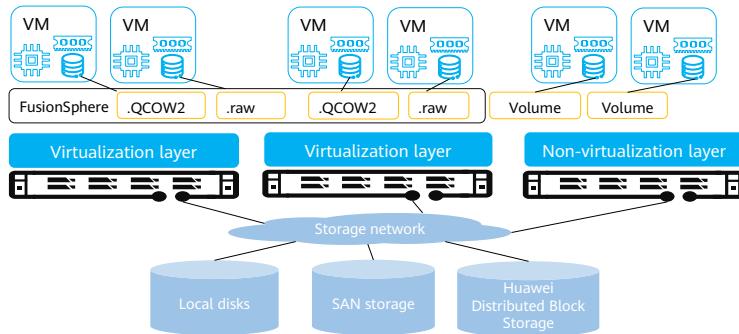
14      Huawei Confidential



- Storage device performance varies, and the interface protocols used by storage devices are different. To address the issues, the storage virtualization technology is used to aggregate resources from different storage devices and provide data stores to manage the resources with the simplicity of a single storage device. Data stores can be used to store VM disk data, VM configuration information, and snapshots.
- VM disks and snapshots are stored as files on data stores. All service-related operations can be converted to operations on files, which enables visibility and agility.
- Based on the storage virtualization technology, Huawei provides multiple storage services to improve storage utilization, reliability, maintainability, and user experience.
- Huawei provides host-based storage virtualization, hiding the complexity of storage device types and bypassing the performance bottlenecks. Storage virtualization abstracts the storage devices as logical resources, thereby providing comprehensive and unified storage service. This feature hides the differences of physical storage devices and provides unified storage functions.

## FusionCompute Functions - Virtual 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.



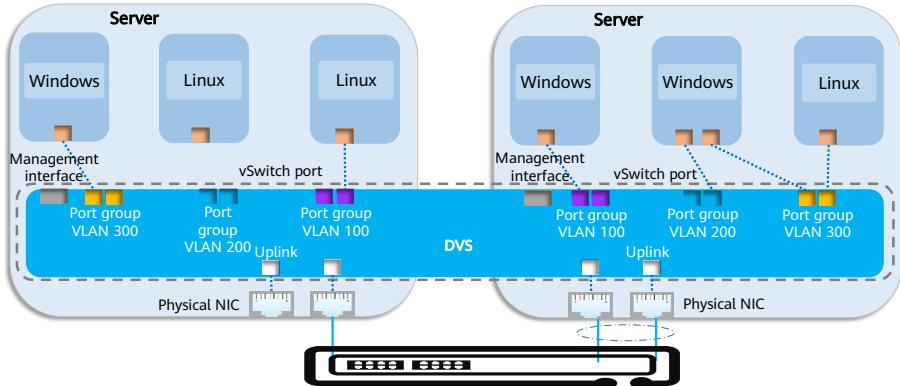
15      Huawei Confidential



- End users can use these virtual volumes on VMs like using local disks on x86 servers. For example, they can format these virtual volumes, read data from or write data into them, install file systems, and install OSs. Moreover, virtual storage supports the snapshot function and resizing, which cannot be implemented on physical disks.
- Administrators only need to manage the SAN devices, instead of managing specific disks. Because SAN devices are reliable, the workloads for replacing disks are significantly decreased for administrators. In addition, virtual storage supports various features that are not supported by physical disks, such as thin provisioning, QoS, and migration. Therefore, virtual storage has distinct cost advantages over physical disks.

## 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.

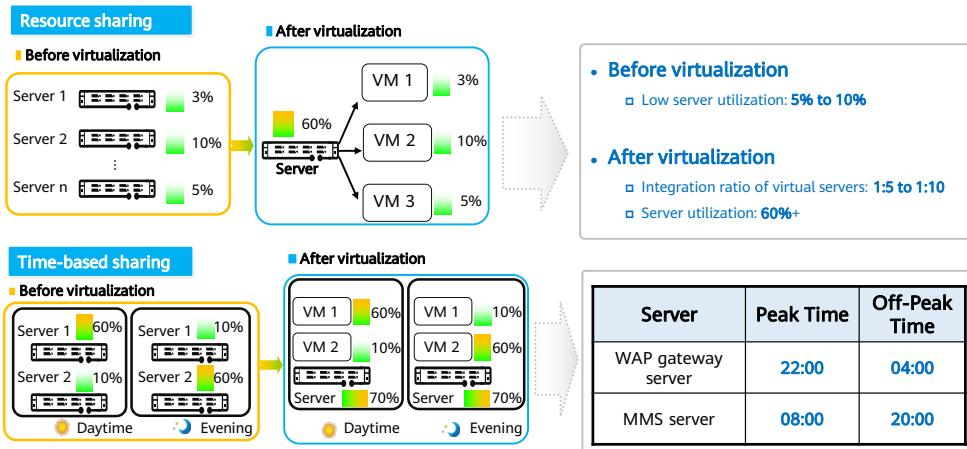


16      Huawei Confidential



- A DVS functions as a physical switch that connects to each host. 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 between all associated hosts. This function ensures network configuration consistency during cross-host VM migration.

## Benefits of FusionCompute (1)

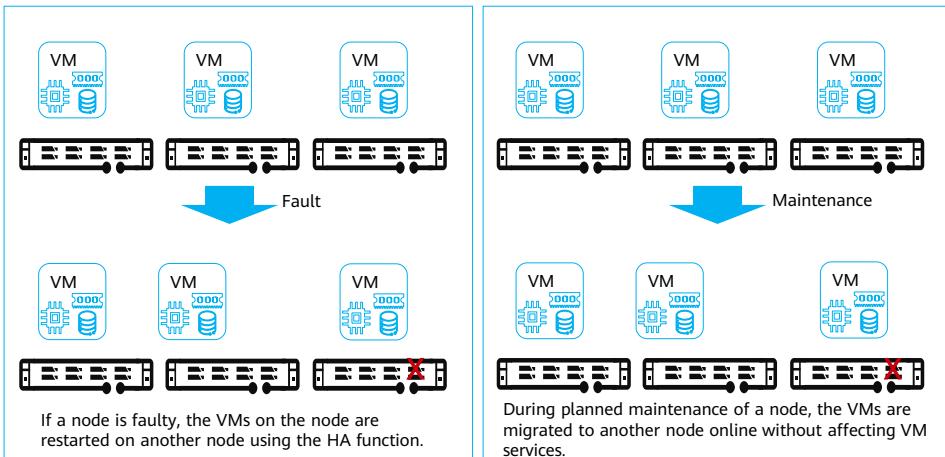


17 Huawei Confidential



- Resource sharing
  - Before virtualization, each physical machine runs an independent application. The resource utilization and return on investment (ROI) is low.
  - After virtualization, the three applications run on one server, which greatly reduces the number of servers to be purchased, and improves the server resource utilization as well as ROI.
- Time-based sharing
  - Before virtualization, applications run on different servers. When the service load of an application on a server is heavy, a server with light service load cannot transfer remaining computing resources to the server. As a result, servers are not used in a balanced manner.
  - After virtualization, applications share all server resources in the system. If the service load of an application on a server is heavy and that on another server is light, FusionCompute allows servers to dynamically assign resources to each application, thereby fulfilling service load requirements and improving the high utilization of the server resources.
- Through explaining the resource sharing and time sharing, it indicates that the resource virtualization can improve resource utilization, lower investment cost, and improve ROI.

## Benefits of FusionCompute (2)



- FusionCompute provides VM high availability (HA) function which will be described in the next course.
- If a host where VMs are located is faulty or needs manual maintenance, FusionCompute can detect the fault in real time and restart the VMs on another normal hosts in a cluster, thereby ensuring service continuity.
- FusionCompute balances workload among hosts through intelligent algorithms, thereby improving the system reliability.
- In summary, if FusionCompute is used and reasonably configured, the system and service operation reliability can be significantly improved.

# Contents

1. Introduction to FusionCompute
2. **FusionCompute Planning and Deployment**
  - Installation Preparation and Network Planning
  - Installation Process and Deployment Solution

# Installation Preparation



## PC or laptop

- Memory: > 2 GB
- Excluding the partition for the OS, at least one partition has more than 15 GB free space.
- OS: 32-bit or 64-bit OSs of Windows 7, Windows 10, Windows Server 2008, Windows Server 2012, and later versions

## Server (CNA)

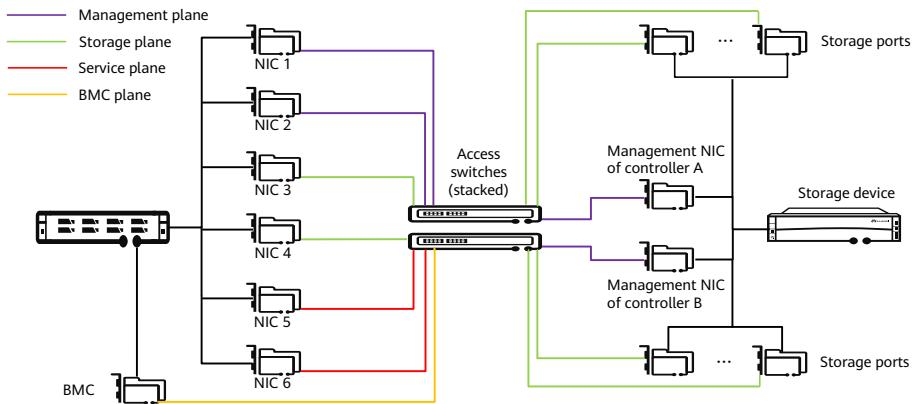
- The CPU supports hardware virtualization technologies, such as Intel VT-x, and the BIOS system must have the CPU virtualization function enabled.
- Memory: > 8 GB (recommended memory size: ≥ 48 GB)
- For compute nodes, the local disk size is greater than 90 GB in the x86 architecture or 110 GB in the Arm architecture so that the server OS can be installed. For management nodes, it is recommended that the local disk space be greater than or equal to 140 GB.

## Precautions

- Do not change the local PC IP address during the installation process.
- Disable the firewall on the local PC before installing FusionCompute.
- Ensure that the file path does not exceed 256 characters.
- Do not restart the host if not required during the installation process.

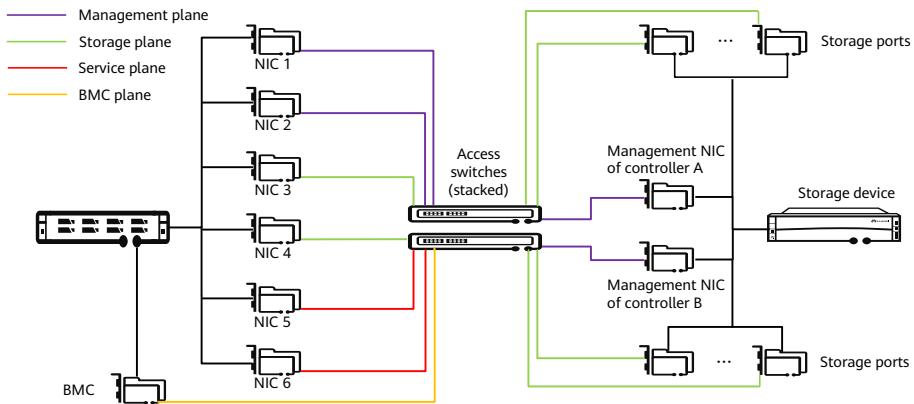
- Ensure that the local PC meets the FusionCompute installation requirements.
- Download the software package from <https://support.huawei.com/enterprise/en/index.html>.
- For product documentation, visit <https://support.huawei.com/hdex/do?docid=EDOC1100215353&lang=en>.

# Network Planning



- BMC plane
  - Specifies the plane used by the baseboard management controller (BMC) network port on a host. This plane enables remote access to the BMC system of a server.
- 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 address of storage device controllers

# Network Planning

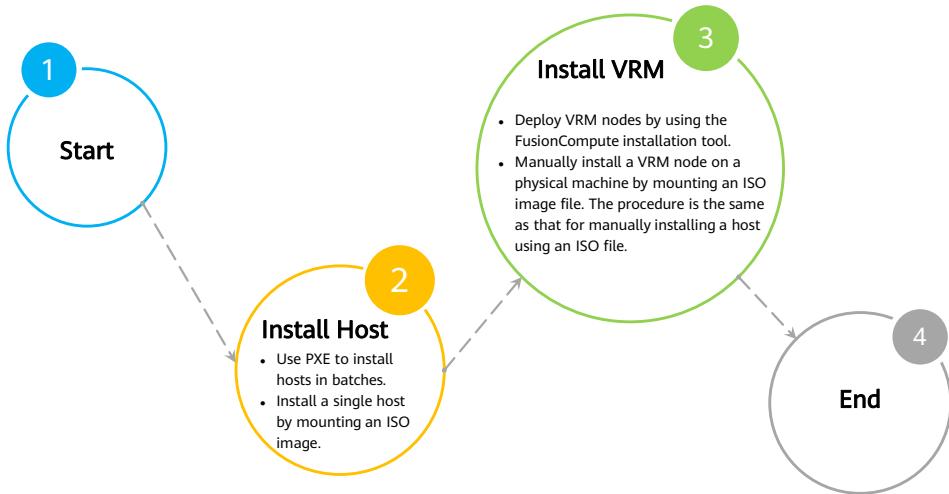


- Storage plane
  - Specifies the plane on which hosts communicate with storage units on storage devices. The storage plane provides the following IP addresses:
    - Storage IP addresses of all hosts, that is, IP addresses of the storage network ports on hosts
    - Storage IP addresses of storage devices
- Service plane
  - Specifies the plane used by user VMs.

# Contents

1. Introduction to FusionCompute
2. **FusionCompute Planning and Deployment**
  - Installation Preparation and Network Planning
  - Installation Process and Deployment Solution

## Installation Process



- Trainees only need to learn and understand the slide content.
- A VRM node can be installed on a physical server using an ISO image file or on a VM accommodated by a CNA host using the installation tool. This task provides guidance for the administrator to install a VRM node on a physical server by mounting an image file. If two VRM nodes are deployed on one site, configure the active/standby mode of the VRM nodes.
- For details, see the experiment manual.

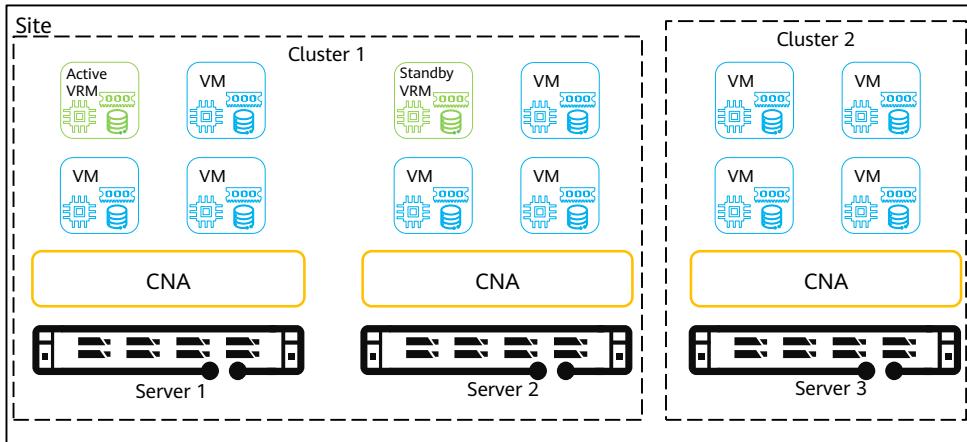
# FusionCompute Deployment Solution

Node	Remarks	
VRM	A management node that supports centralized management of the virtual resources through a management interface.	
CNA	A physical server that provides compute resources for FusionCompute. A host also provides storage resources when local disks are used for storage.	

Node	Deployment Mode	Deployment Principle
Host	Deployed on physical servers	Multiple hosts can be deployed based on customer requirements for compute resources. A host also provides storage resources when local disks are used for storage. When VRM nodes are deployed on VMs, a host must be specified for creating a VRM VM. If a small number of hosts (fewer than 10 hosts) are deployed, you can add all the hosts to the management cluster to provide 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 DVSSs and data stores for hosts in the same cluster.
	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 nodes on VMs.
VRM	Deployed on physical servers	The active and standby VRM nodes must be deployed on different physical servers.

## Logical View of VRM Nodes Deployed on VMs

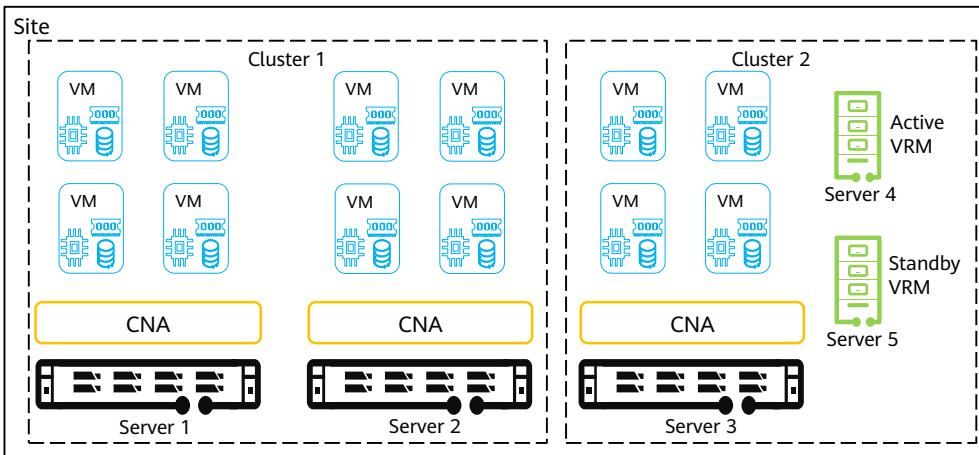


26 Huawei Confidential



- If the active and standby VRM nodes are deployed on different CNAs, the VRM nodes cannot be migrated after being deployed.

## Logical View of VRM Nodes Deployed on Physical Servers



# Quiz

1. Which products are included in the FusionCompute virtualization suite?
  - A. FusionCompute
  - B. FusionCompute Pro
  - C. eBackup
  - D. UltraVR
2. What are the benefits of FusionCompute?
  - A. Enhanced resource utilization
  - B. Improved system availability
  - C. Lower TCO
  - D. Green and energy saving

- Answers:

- ABCD
  - ABCD

# Summary

In this course, we covered the following aspects of FusionCompute:

- Basic concepts
- Architecture and positioning
- Features and functions
- Planning and deployment

In the next course, we will learn how to manage and use FusionCompute.

## Recommendations

- Huawei iLearning
  - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Support Case Library
  - <https://support.huawei.com/enterprise/en/knowledge?lang=en>

## Acronyms and 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.

Copyright©2021 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



# Huawei Virtualization Platform Management and Usage



# Foreword

- FusionCompute is a cloud OS software that virtualizes hardware resources and centrally manages virtual, service, and user resources. This course describes the compute, storage, and network virtualization features, as well as platform management and usage of FusionCompute.

- FusionCompute is a cloud OS software that virtualizes hardware resources and centrally manages virtual, service, and user resources. It uses compute, storage, and network virtualization technologies to virtualize compute, storage, and network resources. 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 cloud data centers.

# Objectives

Upon completion of this course, you will be able to understand the following aspects of FusionCompute:

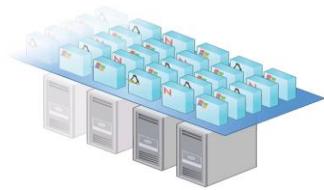
- Compute virtualization features.
- Storage virtualization features.
- Network virtualization features.
- FusionCompute platform and resource management.

# Contents

- 1. Introduction to FusionCompute Compute Virtualization**
  - Concepts Related to Compute Virtualization
    - FusionCompute Compute Virtualization Features
2. Introduction to FusionCompute Storage Virtualization
3. Introduction to FusionCompute Network Virtualization
4. FusionCompute Virtualization Platform Management

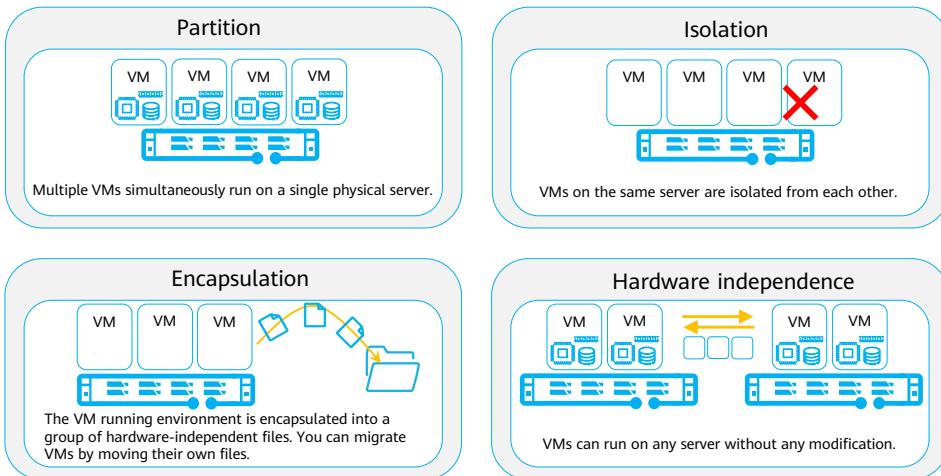
## Introduction to Virtualization

- Virtualization is an abstract layer used to separate physical hardware and OSs.
- Virtual infrastructure is an enterprise-level solution that provides smooth, powerful computing capabilities, maximizing resource utilization and minimizing costs.
- A virtual machine (VM) is an important element in the virtual infrastructure. Virtualization allows multiple VMs with different OSs and applications to run on the same physical machine independently and concurrently.
- With virtualization, users can dynamically adjust resources and processing capabilities as needed.



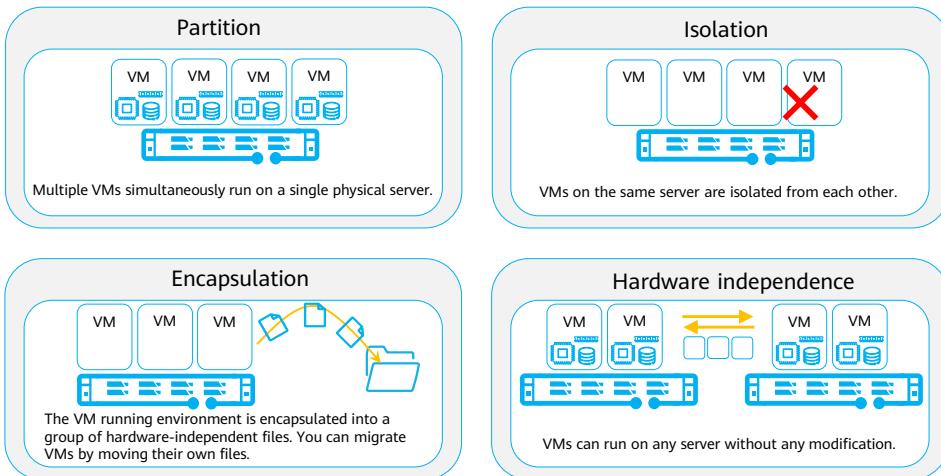
- We have introduced the virtualization technologies in the previous course. Here, let's review the concepts.

# Characteristics of Virtualization



- **Partition:** The virtualization layer allocates server resources to multiple VMs. Each VM can run an independent OS (same as or different from the OSs running on other VMs on the same server) so that applications can coexist on one server. Each OS gains access only to its own virtual hardware (including the virtual NIC, virtual CPUs, and virtual memory) provided by the virtualization layer.
- **Isolation:** VMs that run on the same server are isolated from each other.
  - Even if one VM crashes due to an OS failure, application breakdown, or driver failure, it will not affect the others on the same server.
  - It seems that each VM locates at an independent physical machine. If a VM is infected with worms or viruses, the worms and viruses are isolated from other VMs.
  - 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, leaving no available resources for other VMs in the same system.
  - Multiple loads, applications, or OSs can run concurrently on one physical machine, preventing problems that may occur on the x86 server, for example, application program conflicts or DLL conflicts.

# Characteristics of Virtualization



- **Encapsulation:** Each VM is saved into a group of hardware-independent files, which contain the hardware configuration, BIOS configuration, memory status, disk status, and CPU status. This enables users to clone, save, and migrate VMs by copying, saving, and migrating their own files.
- **Hardware independence:** VMs run on the virtualization layer. Therefore, 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, etc.) without any modification. This breaks the constraints between OSs and hardware and between applications and OSs/hardware.

# Virtualization Technologies

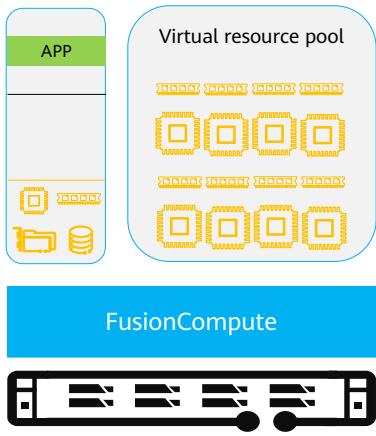
- CPU virtualization
  - FusionCompute uses the Kernel-based Virtual Machine (KVM) technology for compute virtualization. KVM is a CPU-based hardware-assisted virtualization solution that requires CPUs to support the virtualization function.
- Memory virtualization
  - The actual physical memory of a 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.

# Contents

- 1. Introduction to FusionCompute Compute Virtualization**
  - Concepts Related to Compute Virtualization
  - **FusionCompute Compute Virtualization Features**
2. Introduction to FusionCompute Storage Virtualization
3. Introduction to FusionCompute Network Virtualization
4. FusionCompute Virtualization Platform Management

## VM Resource Management – Online CPU and Memory Adjustment



### Working principle

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

### Technical highlights

- Users are allowed to modify CPUs and memory sizes for a running VM. New settings take effect without VM restart.

### Application scenario

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

### Benefits

- 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.
- New settings take effect after VMs are restarted.

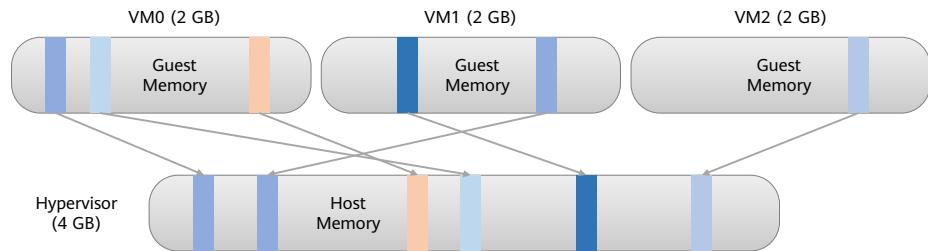
## VM Resource Management – CPU QoS

- This feature allows IT administrators to set an upper limit of resources, preventing non-critical applications or malicious users from preempting shared resources.
- The CPU QoS ensures allocation of compute resources for VMs and prevents cross-VM resource contention caused by service requirements. In short, it increases resource utilization and reduces costs.
- When VMs are created, the CPU QoS is specified based on to-be-deployed services. 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): The CPU QoS ensures allocation of compute resources for VMs. It increases resource utilization and reduces costs.
- CPU QoS includes the following aspects:
  - **CPU quota:** defines the proportion based on which CPU resources are 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 CPU resources to be occupied by a VM.

## VM Resource Management – Host Memory Overcommitment

- Host Memory and Guest Memory are not in a one-to-one relationship.
- Virtual memory that exceeds the actual available memory can be allocated to VMs.
- Memory overcommitment supports such allocation:
  - For example, the physical memory is 4 GB, while the memory of the three upper-layer guest OSs reaches 6 GB.

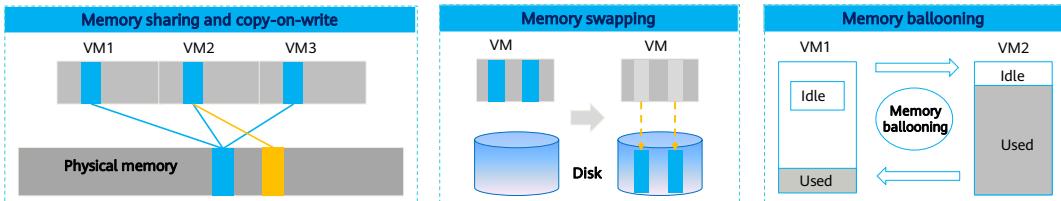


12    Huawei Confidential



- This feature allows a VM to use more memory space than the actual memory space the physical host has by using technologies, such as memory ballooning, memory sharing, and memory swapping.

# VM Resource Management – Memory Overcommitment



Memory sharing: Multiple VMs share the same physical memory block (blue), and the VMs only read data from the memory block.

Copy-on-write: When a VM needs to write data to its memory block, another memory block (orange) is allocated to the VM to write the data, and the mapping between the allocated block and the VM is created.

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 reclaims the unused memory of a VM and allocates it to other VMs to use, improving memory usage.

## Technical highlight

- Huawei virtualization platform increases the memory overcommitment ratio to 150% using these memory overcommitment technologies.

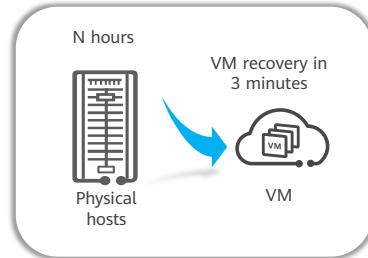
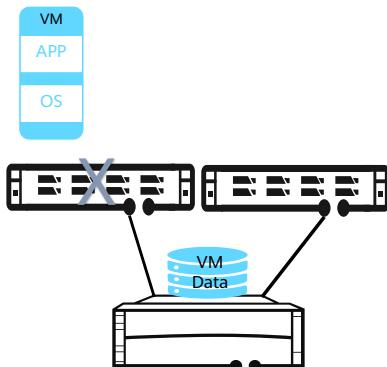
## Benefits

- For a given amount of memory, the VM density is increased by 150%, and the hardware costs are reduced by 50%.

- 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 memory assigned to VMs deployed 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 HA

- This feature ensures a VM, if faulty, can recover quickly. It allows the system to automatically recreate the VM on another normal compute node.

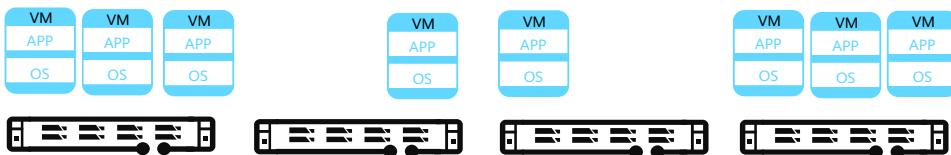


This feature greatly improves the fault recovery speed, shortens the service interruption duration, ensures service continuity, and implements automatic system maintenance.

- HA supports fault detection for hosts, the virtualization platform, and VMs, and VM recovery.
- Centralized HA and VRM-independent HA are supported.
- You can configure the network plane for HA heartbeat messages to mitigate network pressure.
- Multiple fault identification mechanisms are provided to ensure accurate fault locating.
- VM HA can be achieved using a combination of shared and local storage.

## Dynamic Resource Scheduling

- Dynamic resource scheduling (DRS) uses intelligent load balancing and scheduling algorithms to periodically monitor the load on hosts in a cluster. It migrates VMs between the hosts based on the load, achieving load balancing and minimizing power consumption.



### Technical highlights

- In the same cluster, the system automatically balances VM loads based on policies.
- The load balancing algorithm is optimized to prevent invalid VM migration.

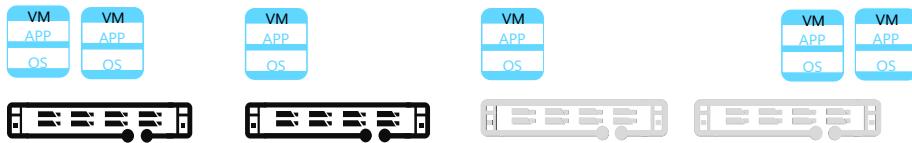
### Application scenarios

- Load balancing is required to ensure service performance.
- Peak clipping is required to avoid congestion during peak hours.

- DRS is also called compute resource scheduling automation.
- FusionCompute computing clusters are deployed on VIMS shared storage devices. DRS monitors resource usage for each compute node in a cluster in real time, and uses the vMotion function to intelligently migrate VMs with high workloads to other nodes with sufficient resources, thereby balancing resource use and ensuring sufficient resources. Therefore, DRS is the basis for 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 physical hosts and allocates VMs evenly on the 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.

## Distributed Power Management

- The automated power management function enables the system to periodically check resource usage on hosts in a 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 idle 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.



### Technical highlights

- The system automatically powers on or off proper physical servers, thereby reducing the number of migrated VMs.
- Some physical servers can be hibernated to wait for new service requirements.

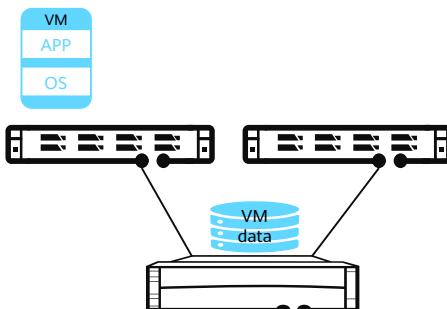
### Application scenarios

- Off-peak light loads (night): Automatically migrate VMs and power off idle hosts.
- Peak production (daytime): Automatically power on hosts and migrate VMs to the hosts.

- The automated power management function enables the system to periodically check resource usage on hosts in a 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 idle 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.

## VM Live Migration

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



### Technical highlights

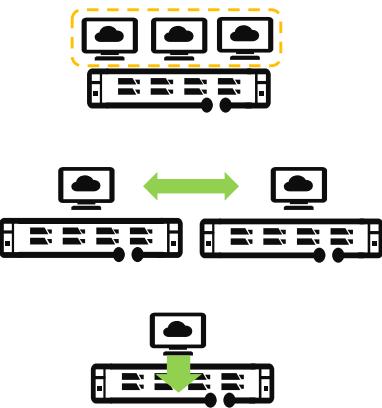
- The memory compression technology improves the VM live migration efficiency by one time.
- The data store location for VM disks remains unchanged, and only the mapping relationship is changed.

### Application scenario

- Services that tolerate short-time interruption but must be quickly restored, such as lightweight database services and desktop cloud services.

- This feature allows VMs to be live migrated from one server to another without interrupting usage or services. Therefore, planned server maintenance will not interrupt applications.
- VM live migration is the basis of dynamic resource scheduling and distributed power management.
- Before performing O&M operations on a physical server, system maintenance engineers can migrate VMs from this physical server to other servers. This minimizes the risk of service interruption during the O&M process.
- Before upgrading a physical server, system maintenance engineers can migrate VMs from this physical server to other servers. This minimizes the risk of service interruption during upgrade. After the upgrade is complete, migrate the VMs back to the original physical server.
- System maintenance engineers can migrate VMs from a light-loaded server to other servers and then power off the server to reduce service operation costs.

## Rule Group



### Keep VMs together

- This rule keeps the selected VMs always running on the same host.

### Keep VMs mutually exclusive

- This rule keeps the selected VMs running on different hosts.

### VMs to hosts

- This rule determines whether the VMs in the specified VM group can run on the specified host in the host group.

- A rule group can define the location relationship between VMs and between VMs and hosts, meeting different application scenarios.

# Contents

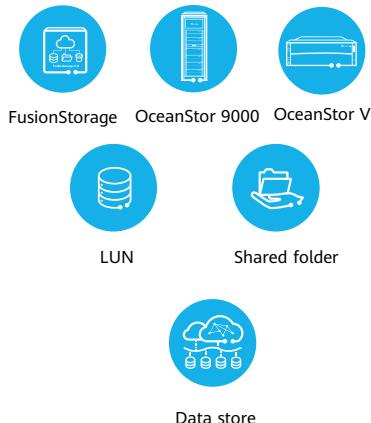
1. Introduction to FusionCompute Compute Virtualization
2. **Introduction to FusionCompute Storage Virtualization**
  - Concepts Related to Storage Virtualization
  - FusionCompute Storage Virtualization Features
3. Introduction to FusionCompute Network Virtualization
4. FusionCompute Virtualization Platform Management

## Introduction to Storage Virtualization

- Storage virtualization abstracts storage devices to data stores so that each VM can be stored as a group of files in a directory on a data store. A data store 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.

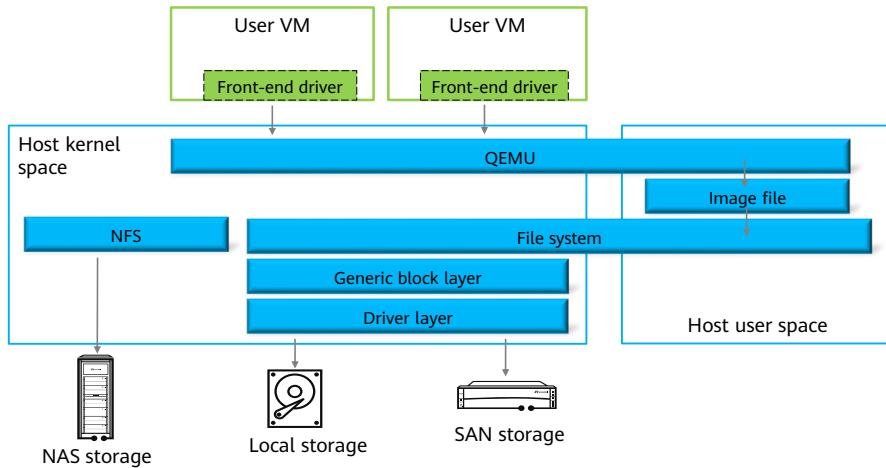
# Storage Concepts in FusionCompute

- Storage resource
  - Indicate physical storage devices, such as IP SAN storage, FusionStorage, and NAS storage.
- Storage device
  - Indicates management units in the storage resource, such as a logical unit number (LUN), a FusionStorage storage pool, or a shared NAS directory.
- Data store
  - Indicates manageable and operable logical units in a virtualized system.



- Huawei aims to build a highly competitive virtualization platform for telecom carriers using the FusionCompute storage virtualization technology. This technology is based on the open-source KVM that has been optimized in terms of security, functions, performance, and reliability and provides the following features:
  - FusionCompute is compatible with various storage devices, including IP SAN, FC SAN, and NAS storage devices, and local disks. It offers file-level service operations.
  - FusionCompute provides comprehensive functions, such as thin provisioning disks, incremental snapshots, cold and hot data migration, linked cloning, and VM disk capacity expansion.
  - Services are running at the virtualization layer. FusionCompute provides homogenous capability even when different storage devices are used at the underlying layer and has no special requirements for storage devices.

## FusionCompute Storage Virtualization Architecture



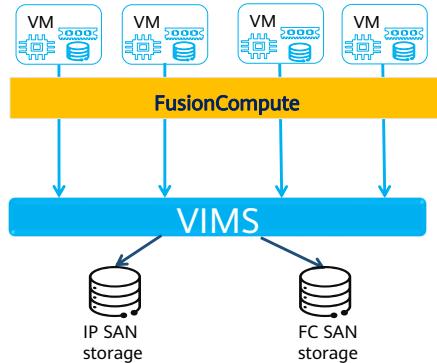
22 Huawei Confidential



- 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.

## Virtual Cluster File System – VIMS

- Virtual Image Management System (VIMS) is a high-performance cluster file system that enables storage resources to be used across storage systems and multiple VMs to access an integrated storage pool, significantly improving resource utilization. The VIMS, as the basis for virtualizing multiple storage servers, provides services such as live migration, DRS, and HA for storage devices.

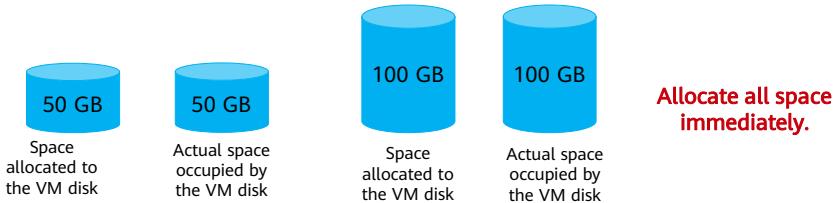


## FusionCompute Disk Technologies

- In storage virtualization, user storage is presented as files. VM disks, snapshots, and VM configurations correspond to independent files.
- In terms of file configuration mode, disks include:
  - Common disk
  - Thick provisioning lazy zeroed disk
  - Thin provisioning disk
- In terms of data security, disks include:
  - Persistent disk
  - Non-persistent disk

## Common Disk

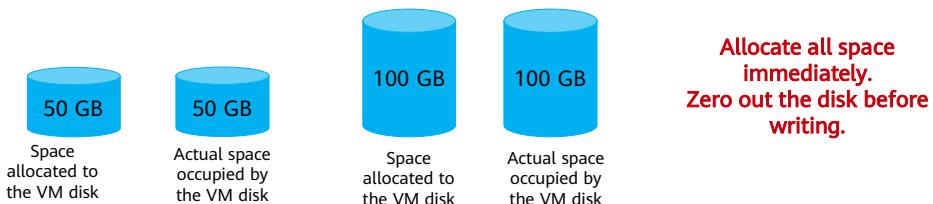
- The size of a common disk is the same as that of a virtual disk. The value 0 is entered for all file locations. Such disks occupy large space and take long space provisioning time.
- On FusionCompute, the disks created in common mode are fixed disks. During creation, the system allocates disk space and zeros out data remaining on the physical device for excellent performance and data security. Creating a common disk takes longer than creating other disks. Common disks are used to meet high input/output operations per second (IOPS) requirements.



- During disk creation in common mode, the system allocates disk space immediately and enters the value 0 for all file locations.

## Thick Provisioning Lazy Zeroed Disk

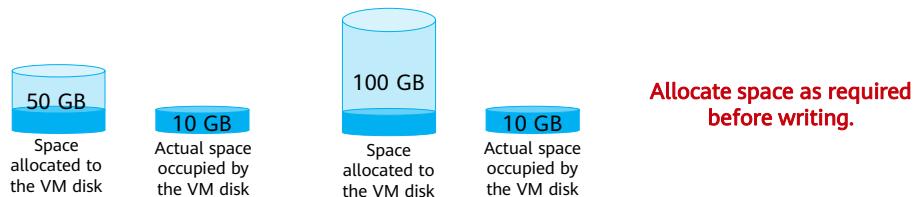
- The size of a thick provisioning lazy zeroed disk is the same as that of a virtual disk. The value 0 is not entered. Such disks occupy large space and take shorter space provisioning time than that required by common disks.
- On FusionCompute, the disks created in thick provisioning lazy zeroed mode can help improve storage utilization. During creation, the system allocates all space but does not zero out data remaining on the physical device, thereby taking less time. Performance of such disks is not as good as that of common disks. Therefore, the thick provisioning lazy zeroed disks apply to scenarios requiring quick provisioning and low IOPS.



- During disk creation in thick provisioning lazy zeroed mode, the system allocates disk space but does not enter the value 0 for all file locations.

## Thin Provisioning Disk

- A new thin provisioning disk contains only a small amount of metadata, just tens of KB. It takes a short time to create such a disk. As users write data, the size of the disk increases according to the actual occupied space.
- On FusionCompute, the disks created in thin provisioning mode can improve storage utilization. Thin provisioning is used to save storage space. The system does not allocate space during disk creation but dynamically allocates space when user I/Os are written into disk files. Performance of such disks is lower than that of common disks. Therefore, the thin provisioning disks are used when users do not have specific storage requirements or the planned capacity is larger than the occupied capacity.

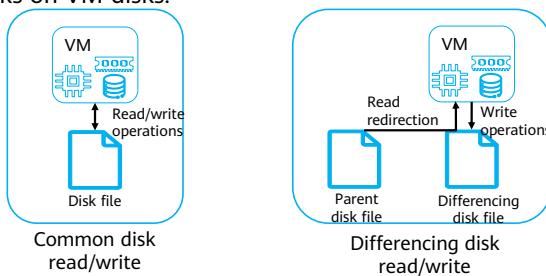


## Persistent and Non-Persistent Disks

- A persistent disk stores data permanently. When an independent persistent disk is created and is not contained in a snapshot, any change is immediately and permanently written to the disk. Snapshot rollback does not roll the data back. The disks can be used to store personal data like a USB flash drive.
- A non-persistent disk stores data temporarily. To protect data on a non-persistent disk, a differencing disk is created for the disk during VM startup. When the VM is running, data changes are written to the differencing disk. After the VM stops, the differencing disk is deleted to restore the non-persistent disk. Non-persistent disks can be used for public computers and for restoring computer data to a previous time point.

## Differencing Disk

- A differencing disk can be created only when a parent disk exists. The differencing disk stores only the differences compared to the parent disk, including data added or deleted. A differencing disk is dependent on a parent disk to be fully functional. If the parent disk is modified, all differencing disks related to it become invalid, and all data written to the differencing disk is lost.
- Differencing disks are used in the snapshot, non-persistent disk, and linked cloning functions of the FusionCompute system to protect the parent disk from being modified and keep track of modified disk blocks on VM disks.



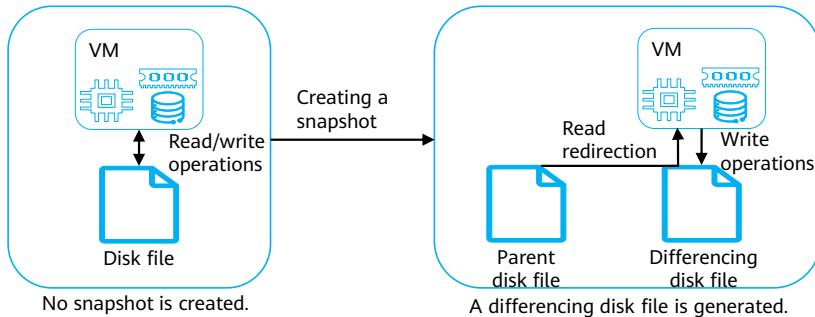
- When a differencing disk is read, the system reads data blocks in the differencing disk first. If the required data does not exist, this data block is not modified. Then the system finds out the parent disk by the file locator in header of the differencing disk and reads data on the parent disk. When a differencing disk is written, all data is written to it.
- The structure of a differencing disk is the same as that of a dynamic disk. The header of a differencing disk contains the pathname of the parent disk. Modified blocks in comparison to the parent disk are stored in the differencing disk. The differencing disk expands dynamically as data is written to it.

# Contents

1. Introduction to FusionCompute Compute Virtualization
2. **Introduction to FusionCompute Storage Virtualization**
  - Concepts Related to Storage Virtualization
  - **FusionCompute Storage Virtualization Features**
3. Introduction to FusionCompute Network Virtualization
4. FusionCompute Virtualization Platform Management

## Snapshot

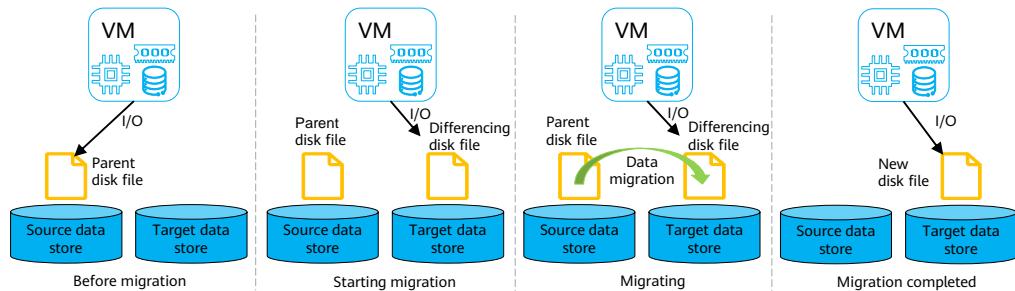
- A snapshot preserves the VM status and data, including disk, memory, and register data. Users can repeatedly revert the VM to any previous states by use of a snapshot. Before performing critical operations, such as system patch installation, upgrade, and, destructive tests, VM users are advised to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



- After a snapshot is created, a differencing disk file is generated and stored in the same directory as the parent disk file. The parent disk file then becomes read-only, and the newly written data is stored in the differencing disk file.
- Data in the differencing disk file is deleted during data rollback by using a snapshot.
- During snapshot deletion, the storage system integrates the data in the parent and differencing disk files to form a new disk file.

## Storage Live Migration

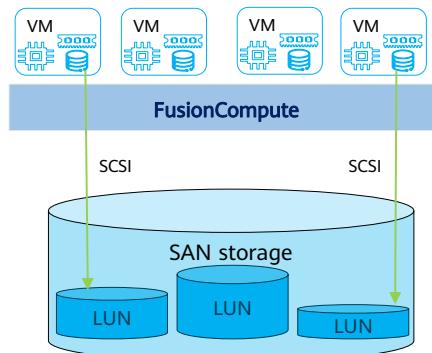
- FusionCompute offers cold migration and live migration for VM disks. Cold migration moves VM disks from one data store to another when the VM is stopped. Live migration moves VM disks from one data store to another without service interruption. The live migration mechanism is as follows:



- To implement live migration, the system first uses the redirect-on-write technique to write VM data to a differencing disk in the target server. Then the parent disk file becomes read-only.
- The data blocks on the parent disk are read and merged into the target differencing disk. After all data is merged, the differencing disk contains all data on the virtual disk.
- The parent disk file is removed, and the differencing disk is changed to a dynamic disk. Then, the disk in the target server can run properly.

## RDM of Storage Resources

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



33      Huawei Confidential



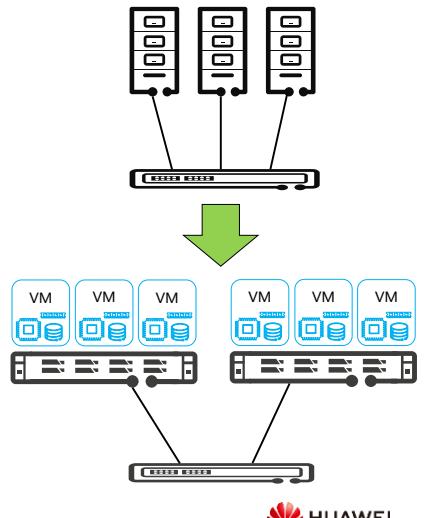
- RDM can bypass a hypervisor layer to transparently transmit the SCSI commands issued by VMs to physical SCSI devices, avoiding function loss due to virtualization layer simulation.
- The following functions are not supported, such as linked cloning, thin provisioning, online and offline capacity expansion, incremental storage snapshot, iCache, storage live migration, storage QoS, disk backup, and VM conversion to a template.
- Technical highlights:
  - VMs directly issue SCSI commands to operate raw devices.
  - FC SAN storage and IP SAN storage support the RDM feature.
- RDM applies to applications that require high-performance storage, such as Oracle RAC.

# Contents

1. Introduction to FusionCompute Compute Virtualization
2. Introduction to FusionCompute Storage Virtualization
- 3. Introduction to FusionCompute Network Virtualization**
  - Concepts Related to Network Virtualization
  - FusionCompute Network Virtualization Features
4. FusionCompute Virtualization Platform Management

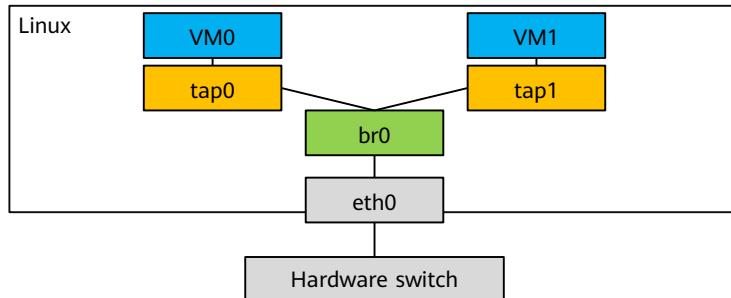
## Development of Network Virtualization

- 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.



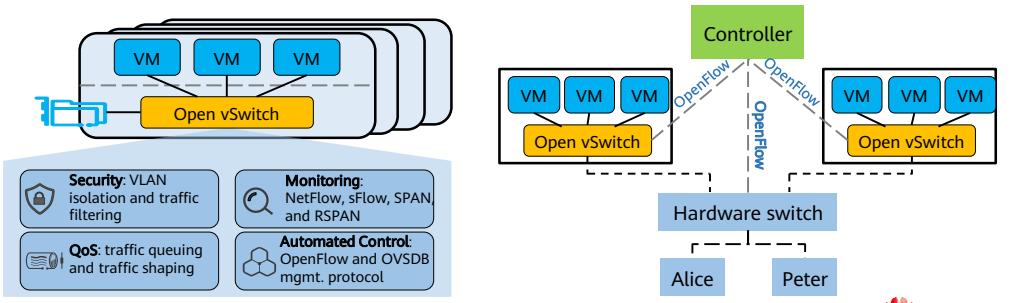
## Introduction to Linux Bridge

- 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.



## 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.



37 Huawei Confidential

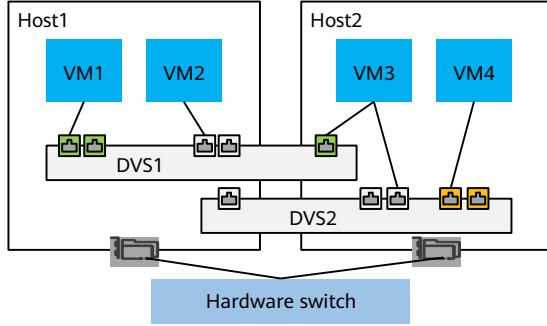


- An Open vSwitch (OVS) is a software-based open-source virtual switch. It complies with the Apache 2.0 license. It supports multiple standard management interfaces and protocols, such as NetFlow, sFlow, SPAN, Remote Switched Port Analyzer (RSPAN), Command Line Interface (CLI), LACP, and 802.1ag. It 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.

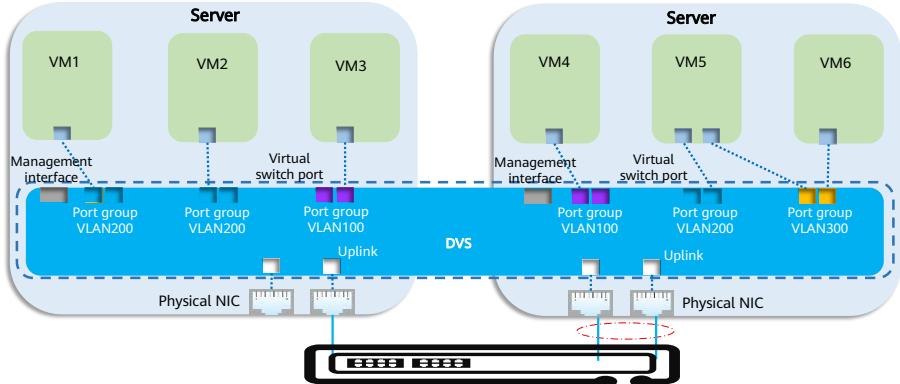
## Introduction to DVS

- 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.



## FusionCompute DVS

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



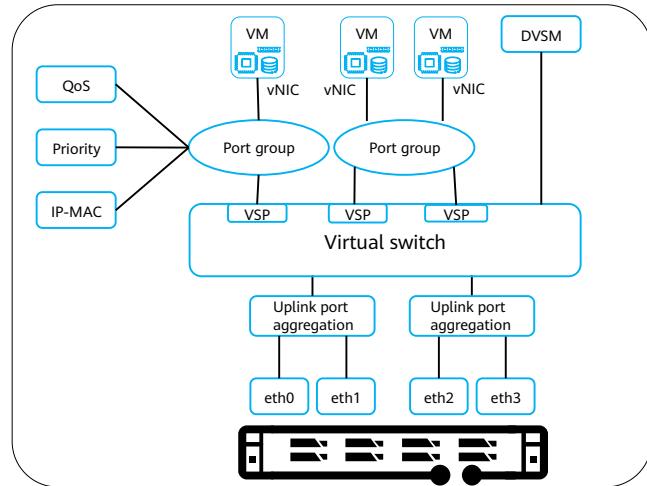
39      Huawei Confidential



- 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

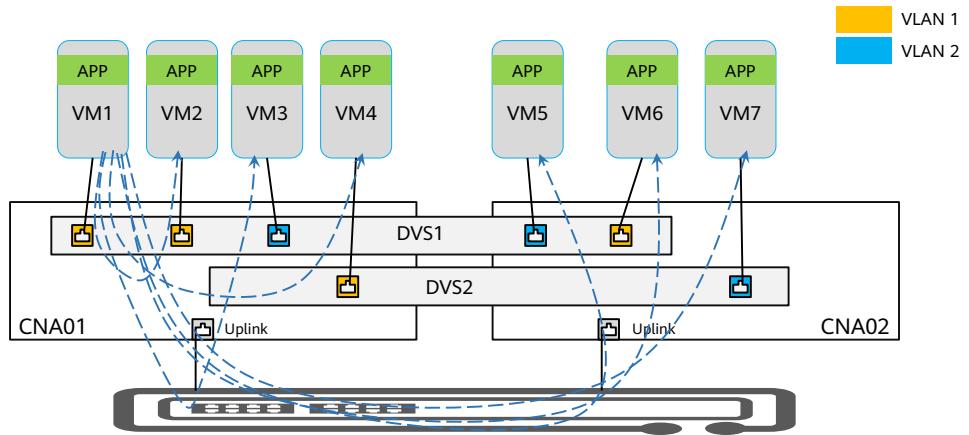


40      Huawei Confidential



- DVSM: Distributed Virtual Switch Manager
- The VM port attributes setting can be simplified by configuring port group attributes, including security and QoS. The port group attributes setting has no impact on the proper running of VMs.
- A port group consists of multiple ports with the same attributes. The VM port attributes setting can be simplified by configuring port group attributes, including bandwidth QoS, layer-2 security attributes, and VLAN. Port group attribute changes do not affect VM running.
- An uplink connects the host and the DVS. Administrators can query information about an uplink, including its name, ratio, mode, and status.
- Uplink aggregation allows multiple physical ports on a server to be bound as one port to connect to VMs. Administrators can set the bound port to load balancing mode or active/standby mode.

## VM Communication on FusionCompute

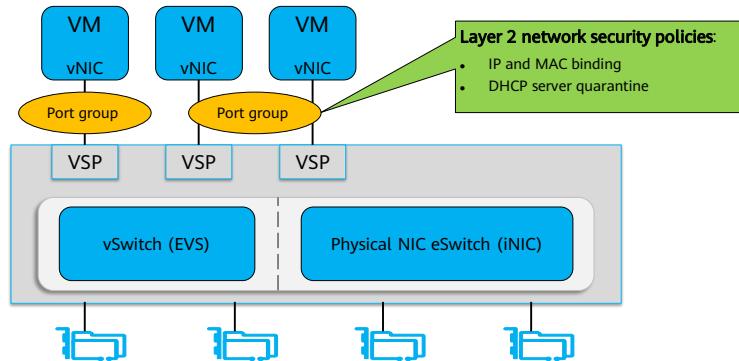


# Contents

1. Introduction to FusionCompute Compute Virtualization
2. Introduction to FusionCompute Storage Virtualization
- 3. Introduction to FusionCompute Network Virtualization**
  - Concepts Related to Network Virtualization
  - FusionCompute Network Virtualization Features
4. FusionCompute Virtualization Platform Management

## 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.



43      Huawei Confidential



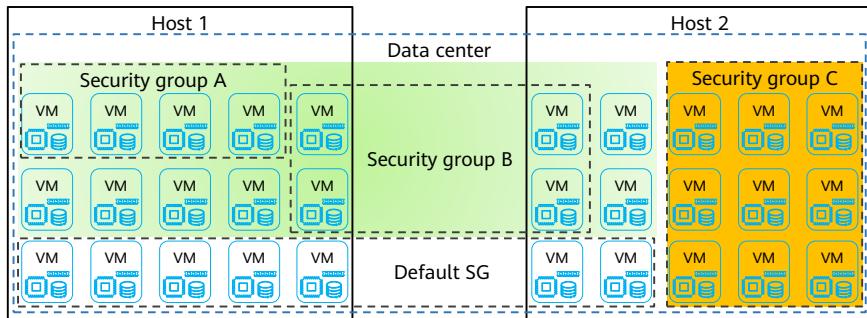
- IP-MAC address binding prevents IP address or MAC address spoofing initiated by changing the IP address or MAC address of a virtual NIC (vNIC), and therefore enhances network security of user VMs. After the binding, the packets from untrusted sources are filtered through IP Source Guard and dynamic 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

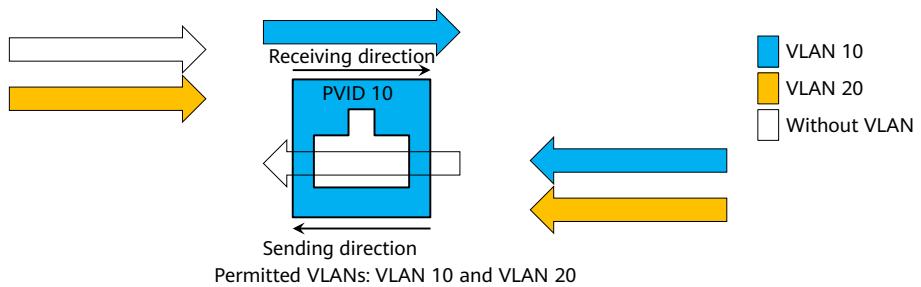
- In server consolidation and desktop cloud scenarios, broadcast packet attacks caused by network attacks or virus may interrupt network communication. To prevent this, broadcast packet suppression is enabled for virtual switches.
- Virtual switches support suppression of broadcast packets sent from 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.



## Trunk Port

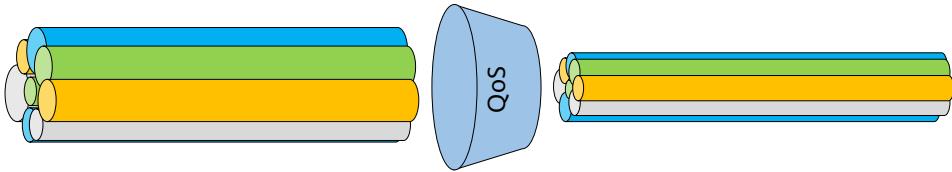


### Trunk port overview

- 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.

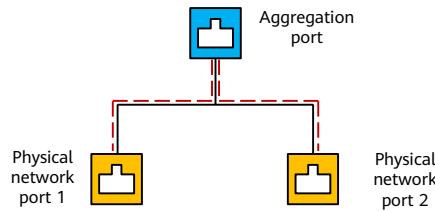
## Network QoS



The network QoS policy enables bandwidth configuration and control, including:

- Bandwidth control based on the directions (sending and receiving) of a port group member
- Traffic shaping and bandwidth priority configured for each member port in a port group

## Binding Network Ports



### Host network port bonding

- On FusionCompute, administrators can bind network ports on a CNA host to improve network reliability.
  - Port binding can be configured for common NICs and DPDK-driven NICs.

- 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

1. Introduction to FusionCompute Compute Virtualization
  2. Introduction to FusionCompute Storage Virtualization
  3. Introduction to FusionCompute Network Virtualization
- 4. FusionCompute Virtualization Platform Management**
- Maintenance and Management
  - Configuration Management
  - Cluster Resource Management

## FusionCompute User 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.

# Alarm Management

Alarm Severity	Icon	Description
Critical	🔴	Indicates a fault that affects the service at present, and needs to be rectified promptly.
Major	🟠	Indicates a fault that affects the service at present, and if not rectified, could result in serious consequences.
Minor	🟡	Indicates a fault that does not affect the service at present, but if not rectified, could result in more severe faults.
Warning	🔵	Indicates a potentially or imminently hazardous fault, that does not affect the service at present.

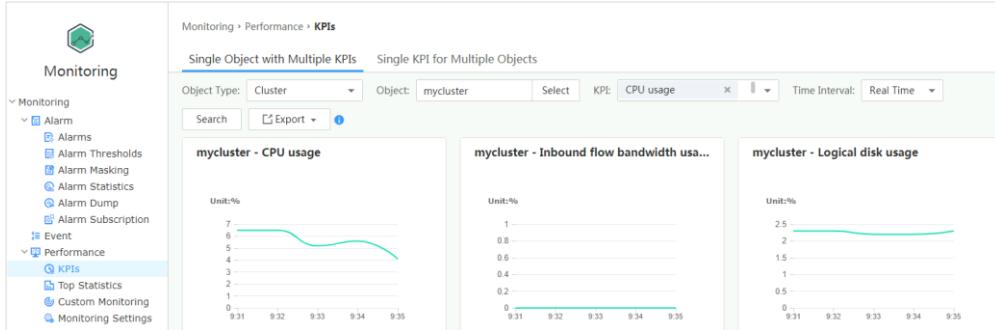
The screenshot shows the 'Monitoring' section of the FusionCompute interface. On the left, there's a navigation tree under 'Monitoring' with 'Alarms' selected. The main area displays a table of 'Real-Time Alarms'. The table has columns: Alarm ID, Alarm S..., Alarm Name, Alarm Object, Object Ty..., Generate Time, Clear Time, Clear Ty..., and Operation. There are five entries in the table, all of which are Major severity level (orange dots). The first four entries are for 'Remote Manage...' objects, and the fifth is for 'Default System C... site'. Each entry includes a 'Clear' button and a 'More' dropdown.

Alarm ID	Alarm S...	Alarm Name	Alarm Object	Object Ty...	Generate Time	Clear Time	Clear Ty...	Operation
15.1007030	Major	Remote Manage...	VRM02	VRM	-	-	Clear	More
15.1007030	Major	Remote Manage...	VRM01	VRM	-	-	Clear	More
15.1007019	Major	NTP Clock Source...	VRM02	VRM	-	-	Clear	More
15.1007033	Major	Default System C...	site	Site	-	-	Clear	More
15.1007019	Major	NTP Clock Source...	VRM01	VRM	-	-	Clear	More

- 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.

# Contents

1. Introduction to FusionCompute Compute Virtualization
2. Introduction to FusionCompute Storage Virtualization
3. Introduction to FusionCompute Network Virtualization
- 4. FusionCompute Virtualization Platform Management**
  - Maintenance and Management
  - Configuration Management
  - Cluster Resource Management

## 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)

The screenshot shows the 'System' configuration page in FusionCompute. The left sidebar has a tree view under 'System':

- Tasks and Logs
  - Task Center
  - Operation Log
  - Log Collection
- Rights Management
  - User Management
  - Role Management
  - Password Policy
  - Domain Authentication
- System Configuration
  - License Management
  - Services and Manager
  - Authentication Mgt.
  - Time Management
  - System Logo
  - Service Configuration
- Connect To
- Network Change

The main panel title is 'System' with the subtitle 'Manage system settings, and view task status and logs.' It contains six icons:

- Tasks and Logs
- Rights Management
- System Configuration
- Service Configuration
- Connect To
- Network Change

- 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.

The screenshot shows the 'Task Center' page within the 'Tasks and Logs' section of the FusionCompute interface. The left sidebar lists various system categories like System, Task Center, Operation Log, Log Collection, Rights Management, User Management, Role Management, Password Policy, Domain Authentication, System Configuration, License Management, Services and Management, Authentication Mgt., Time Management, System Logo, Service Configuration, and Connect To. The 'Task Center' item is selected and highlighted in blue. The main content area displays a table of tasks with the following data:

Task Name	Object Na...	Status	Start Time	End Time	Description
Forcibly Rest...	vDesktop Te...	Successful			
Mount CD/D...	vDesktop Te...	Successful			
Create VM	vDesktop Te...	Successful			
Mount Tools	FA-ITADBHD...	Successful			
Forcibly Rest...	FA-ITADBHD...	Successful			
Mount CD/D...	FA-ITADBHD...	Successful			
Start VM	FA-ITADBHD...	Successful			
Forcibly Stop ...	FA-ITADBHD...	Successful			
Create VM	FA-ITADBHD...	Successful			
Create VM	FA-ITADBHD...	Successful			

# Contents

1. Introduction to FusionCompute Compute Virtualization
2. Introduction to FusionCompute Storage Virtualization
3. Introduction to FusionCompute Network Virtualization
- 4. FusionCompute Virtualization Platform Management**
  - Maintenance and Management
  - Configuration Management
  - Cluster Resource Management

## Cluster Management

Function	Description	Navigation Path
Monitoring clusters	Query cluster monitoring information (for example, running status) of a cluster within the specified time period.	
Configuring cluster attributes	Configure cluster attributes, such as the HA policy, memory overcommitment policy, and VM start policy.	<b>Homepage &gt; Resource Pool &gt; Cluster</b>
Configuring the resource scheduling policy	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

The screenshot shows the Fusion Compute interface for cluster configuration. The left sidebar has icons for Home, Resource Pools, VMs, Hosts, Datastores, and Alarms. The 'Resource Pools' section is selected, showing a tree view with 'mycluster' expanded, containing 'VM Template', 'Folders', 'Storage', 'Network', 'Security Group', and 'GPU Resource Group'. The main panel title is 'Resource Pools > mycluster'. Below it are tabs: Summary, Monitoring, Configuration (selected), Host, VM, Datastore, and Alarm. Under 'Configuration', 'Control Cluster Resource' is selected, showing 'VM Override Policy', 'DRS Advanced Settings', and 'DRS Rule'. The 'DRS Rule' section is expanded, showing four items: 'Basic Configuration' (disabled), 'Configure HA' (enabled), 'Configure Resource Scheduling' (disabled), and 'Configure IMC' (disabled).

- If you want to configure the DRS rule, enable the cluster resource scheduling.

# Host Management

Function	Description	Navigation Path
Monitoring hosts	Query cluster monitoring information (for example, running status) of a cluster within the specified time period.	<a href="#">Homepage &gt; Resource Pool &gt; Host</a>
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.	
Associating storage resources with the host	Associate storage resources with the host to provide storage space for the VM on the host.	<a href="#">Homepage &gt; Resource Pool &gt; Host &gt; Configuration</a>

## Host Management Configuration

The screenshot shows the Fusion Compute interface. In the top navigation bar, there is a search bar with the placeholder "Enter a keyword." Below the navigation bar, there are several buttons: Create VM, Power Off, Restart, Enter Maintenance Mode, More, Summary, Topology, Monitoring, Configuration (which is selected), VM, Datastore, DVS, Task and Event, and Alarm. On the left side, there is a sidebar with icons for Home, Resource Pools, VM Template, Folders, Storage, Network, Security Group, and GPU Resource Group. Under "Resource Pools", there is a tree view: mycluster > cna01 > cna02 > Windows\_2016\_en\_terminator > Windows\_2016\_cn\_terminator > ita02 > ita > Windows\_2016\_cn\_terminator > FA-ITADBHDWCWILIVAG > FA-ITADBHDWCWILIVAG. The "Configuration" tab is active, and under "System Configuration", the "Host Settings" section is selected. This section contains the following configuration items:

Management Domain Resources	9680 (MB)/3 (vCPU)
Hugepage Memory	Disabled
User-mode Switch Specifications	Disabled
BMC Configuration	Not configured
Time Synchronization	Not configured
Antivirus Settings	Disabled

61      Huawei Confidential



- 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.

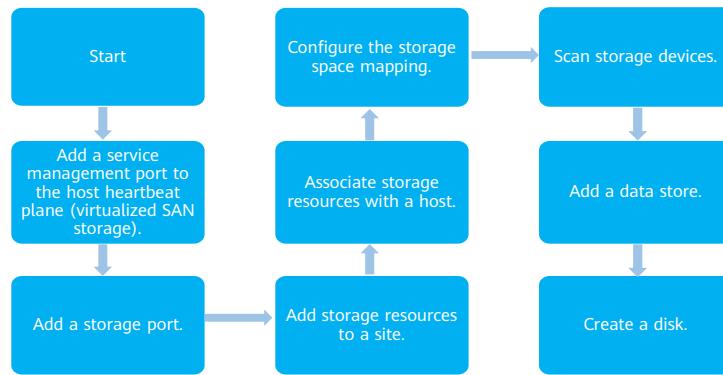
# Host Management Configuration

The screenshot shows the Fusion Compute interface for managing a host named 'cna01'. The left sidebar lists 'Resource Pools' under 'mycluster', including 'cna01', 'cna02', and several VM templates like 'Windows\_2016\_en\_terminator' and 'Windows\_2016\_cn\_terminator'. The main panel shows the 'System Configuration' tab selected. Under 'Host Settings', there are sections for 'Management Domain Resources' (9680 MB/3 vCPU), 'Hugepage Memory' (Disabled), 'User-mode Switch Specifications' (Disabled), 'BMC Configuration' (Not configured), 'Time Synchronization' (Not configured), and 'Antivirus Settings' (Disabled).

- 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.

## 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.



63      Huawei Confidential

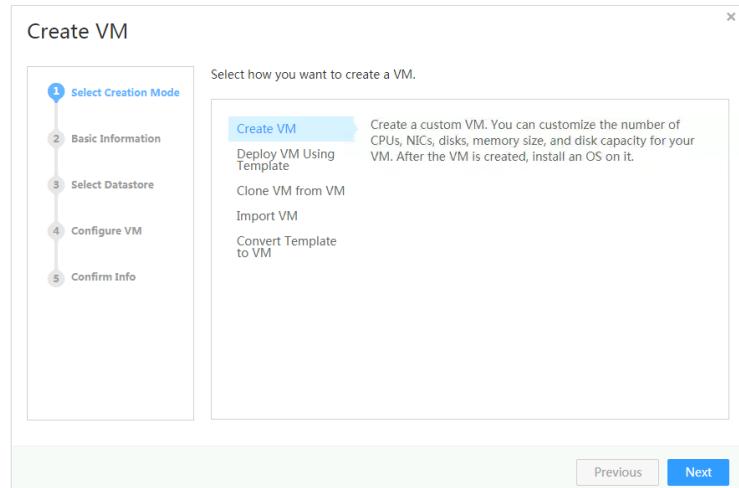


## Network Resource Management

- 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.

## VM Lifecycle Management – Creating a VM



65      Huawei Confidential



- You can create a VM in any of the following ways:
  - Creating a VM
  - Deploying a VM using a VM template
  - Cloning a VM to a VM
  - Importing a VM
  - Converting a template to a VM

## 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.

The screenshot shows the FusionCompute interface for managing VMs. On the left, there's a tree view of 'Resource Pools' under 'mycluster'. The 'cna02' pool is selected, showing several VMs listed in a table. One VM, 'i-00000047', is highlighted. A context menu is open over this VM, with the 'More' option expanded. The 'Clone VM' option is clearly visible and highlighted with a red box.

ID	Status	Type	CPU A...	CPU Usage	Memory Usage	Disk Usage	IP Address	Operation
i-00000003	Running	Common VM	X86	8.04%	79.21%	11.56%	192.168.104.3...	<a href="#">Log In Using VNC</a> More
i-00000050	Running	Common VM	X86	0.0%	0.0%	0.0%	0.0.0.0.0.0.0	<a href="#">Log In Using VNC</a> More
i-00000045	Running	Common VM	X86	0.0%	17.00%	15.08%	0.0.0.0	<a href="#">Log In Using VNC</a> More
i-00000047	Running	Common VM	X86	0.0%	17.20%	12.57%	0.0.0.0	<a href="#">Log In Using VNC</a> More

## VM Lifecycle Management – Powering Off or Deleting a VM

The screenshot shows the vSphere Web Client interface. On the left, the navigation tree displays 'Resource Pools' under 'mycluster' and 'cna02'. The main area shows a table of VMs with columns: ID, Status, Type, CPU A..., CPU Usage, Memory Usage, Disk Usage, IP Address, and Operation. Four VMs are listed: i-00000003, i-00000050, i-00000045, and i-00000047, all in 'Running' status. A context menu is open over the fourth VM (i-00000047), with the 'Power' option highlighted. Other options in the menu include Start, Hibernate, Restart, Forcibly Restart, Stop, Forcibly Stop, Retrieve VM, Migrate, Clone VM, Template, Create Snapshot, and Tools.

ID	Status	Type	CPU A...	CPU Usage	Memory Usage	Disk Usage	IP Address	Operation
i-00000003	Running	Common VM	X86	8.04%	79.21%	11.56%	192.168.104.3...	<a href="#">Log In Using VNC</a> More ▾
i-00000050	Running	Common VM	X86	0.0%	0.0%	0.0%	0.0.0.0.0.0.0	<a href="#">Log In Using VNC</a> More ▾
i-00000045	Running	Common VM	X86	0.0%	17.00%	15.08%	0.0.0	<a href="#">Log In Using VNC</a> More ▾
i-00000047	Running	Common VM	X86	0.0%	17.20%	12.57%	0.0.0	<a href="#">Log In Using VNC</a> More ▾

# Quiz

1. Which benefits does VM migration offer?
  - A. Automatically recovers services when the VM system is faulty.
  - B. Balances the load on each physical server.
  - C. Ensures high system reliability.
  - D. Supports online hardware upgrade.
2. Which of the following are memory overcommitment technologies?
  - A. Memory sharing
  - B. Memory ballooning
  - C. Memory swapping
  - D. Memory thin provisioning

- Answers:

- BCD
  - ABC

# Summary

- In this course, we have learned:
  - Compute, storage, and network virtualization features of FusionCompute
  - Basic operations about the FusionCompute platform, such as resource management
- In the next course, we will learn the development trend of cloud computing technologies.

## Recommendations

- Huawei iLearning
  - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Support Case Library
  - <https://support.huawei.com/enterprise/en/knowledge?lang=en>

## Acronyms and Abbreviations

- DRS: Dynamic Resource Scheduling
- 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.

Copyright©2021 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



## Overview of FusionAccess



# 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

- Upon completion of this course, you will understand:
  - The system architecture, benefits, and features of FusionAccess
  - The functions and principles of HDP
  - The component architecture and application scenarios of FusionAccess

# Contents

- 1. Overview of FusionAccess**
2. Introduction to FusionAccess Components
3. Introduction to HDP
4. Introduction to FusionAccess Application Scenarios

# Requirements for an Age of Informatization

IT capabilities and data assets will become critical to staying competitive.



Gartner:  
IT will transform all companies!

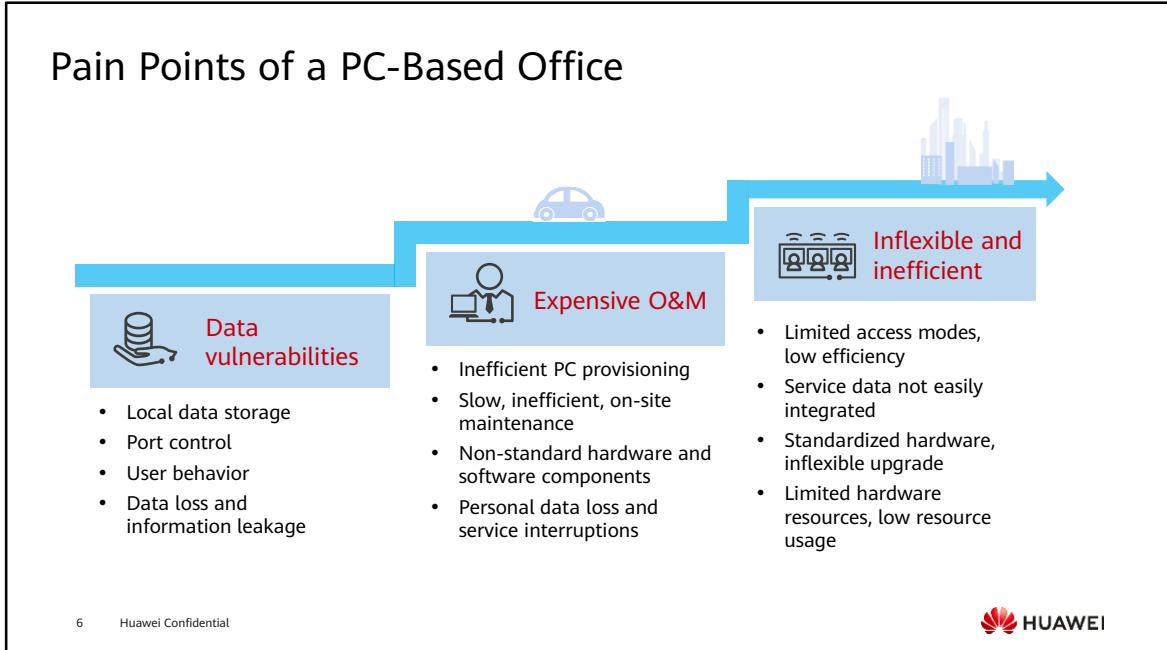
Massive data collaboration  
A wide variety of intelligent terminals

Data protection  
for enterprises and individuals alike

**Requirements: Improve IT system efficiency to turbo-charge business development and ensure information security.**

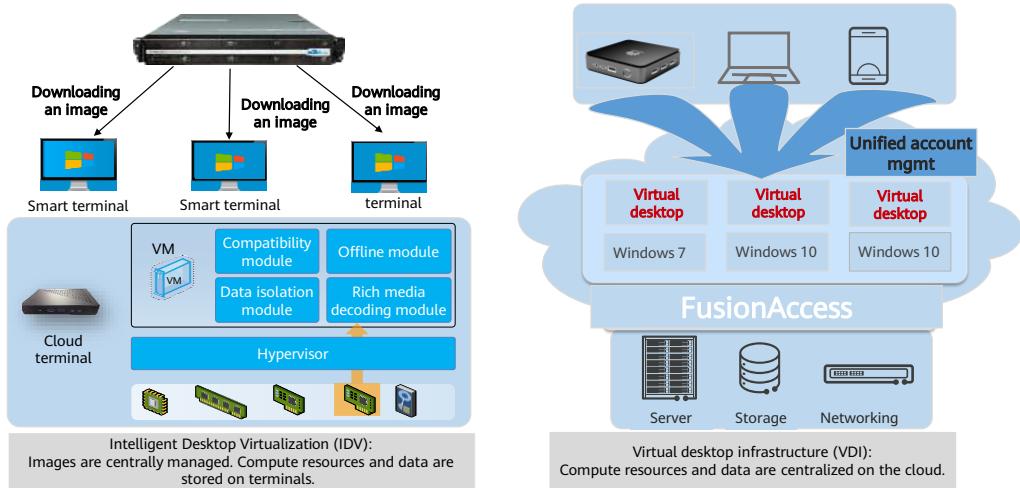
- New technologies, such as cloud computing, big data, mobility, social IT, and the Internet of Things (IoT), are transforming peoples' lives.
  - The Internet is everywhere.
  - Mobile Internet means you can get online anytime from anywhere.
  - You can access information on the cloud, or even work on cloud.
  - Enterprises use big data to analyze services and adjust their strategies.
  - Chatting online has become commonplace.

## Pain Points of a PC-Based Office



- Nowadays, PCs have become essential to enterprise operations, but using PCs for everything has created some problems too.
  - First, there is information security. When all of your data is saved to local PCs, even though a lot of work has gone into keeping this data safe. Data losses and information leakage seem inevitable.
  - Second, PC management and maintenance have also become a burden. As the number of PCs keeps increasing and new applications keep being developed, it makes O&M more complicated and time consuming. And outsourcing IT O&M just drives up OPEX. Time wasted handling PC faults and provisioning new devices slow down service development.
  - Third, physical resources are fixed, which means they often get wasted. PCs tend to be in use only for a third of the day. Once staff leaves work and goes home, those physical PCs are left idle or shut down for the remainder. Their capacity is wasted. Furthermore, when more powerful processing capabilities are required due to service changes, physical PCs fail to keep up due to hardware constraints. PC-based office desktops have become a bottleneck for service development.

## VDI and IDV (1)



7 Huawei Confidential

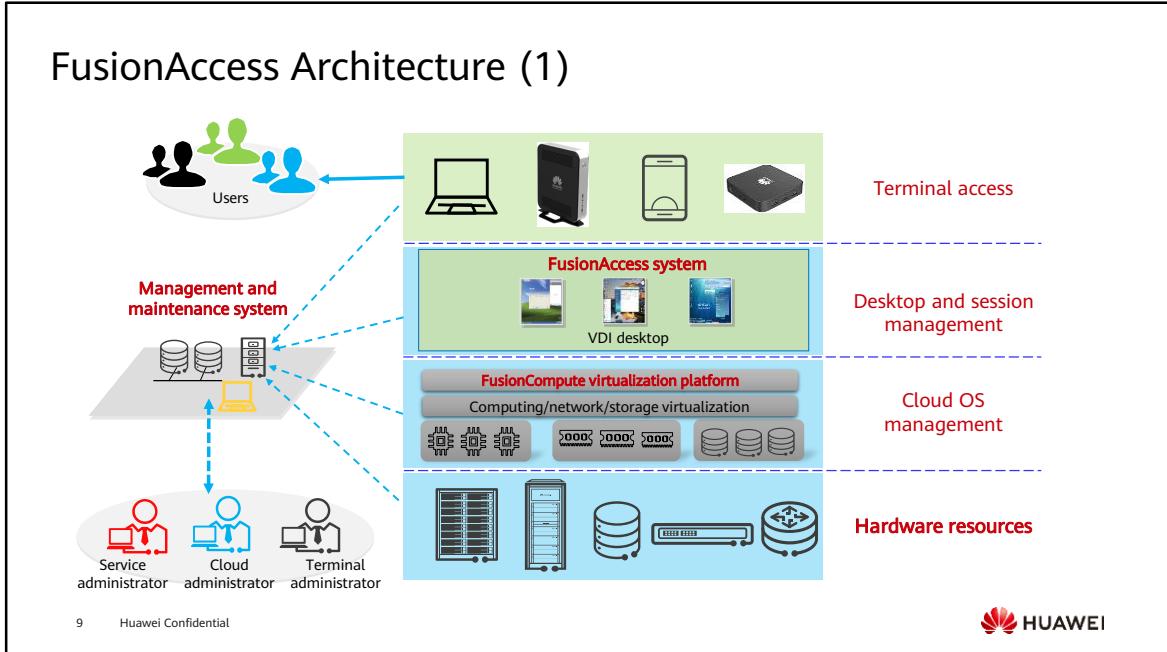


- Technology Comparison
  - An IDV represents a small step forward from a traditional PC-based office architecture. Typically, it consists of an image server, management software, and local virtual desktop terminals (fat clients). A VDI, in contrast, is a completely new design. Instead of PCs, it uses 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.

## VDI and IDV (2)

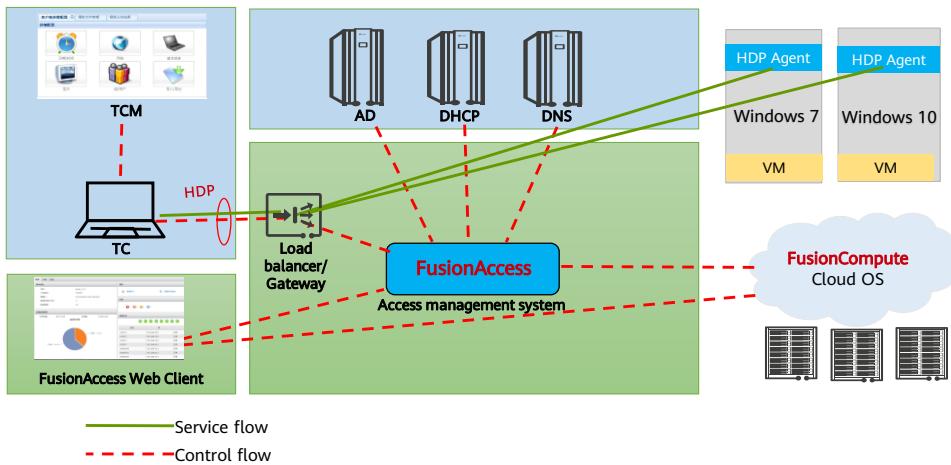
Item	VDI	IDV	Remarks
Data Security	High. Centralized data storage prevents data leakage through terminal access.	Low. Data is downloaded to the terminals, which makes data leakage more likely.	Centralized data storage is more secure than local storage.
Terminal Maintenance	Easy. Terminals only provide 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.

## FusionAccess Architecture (1)



- FusionAccess is a virtual desktop application deployed on hardware and enables end users to access cross-platform applications and virtual desktops from TCs or other networked devices.
- FusionAccess brings higher information security, requires less investment, and improves office efficiency over conventional PCs. It fits into the office automation (OA) of financial institutions, enterprises, public institutions, and medical institutions, and allows you to work smoothly even when you are outdoors or on business trip. FusionAccess ensures the optimal OA user experience anytime, anywhere.
- FusionAccess boasts the following advantages:
  - Administrators can deploy, manage, and maintain virtual desktops, which run in the data center, in a centralized manner.
  - Users can easily access personalized virtual desktops and obtain the PC-like user experience.
  - Total cost of ownership (TCO) is reduced because virtualized desktops require less management and resources.
  - FusionAccess supports GPU passthrough and GPU hardware virtualization, allowing users to remotely access graphics desktops and helping reduce the TCO of graphics desktops.

## FusionAccess Architecture (2)

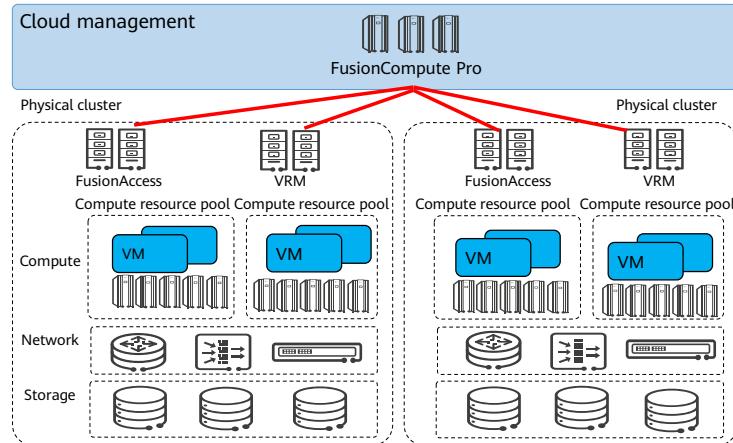


10    Huawei Confidential



- FusionAccess is the proprietary virtual desktop access management system of Huawei. FusionAccess uses the Huawei Desktop Protocol (HDP) to manage virtual desktop services and control permissions.
- The HDP Agent, part of the FusionAccess system, transmits desktop display information of VMs to clients using the HDP and receives peripheral information about the keyboard and mouse of clients.
- FusionCompute is the cloud OS software that virtualizes hardware resources and centrally manages virtual, service, and user resources. It also virtualizes compute, storage, and network resources. 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 and green data centers.
- FusionAccess Web Client is the unified management system developed by Huawei. It is used to manage the FusionAccess desktop services and can be embedded in FusionManager, the FusionCompute management software.

# Cloud Platform Architecture of FusionCompute



11    Huawei Confidential



- 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. It maximizes resource utilization by consolidating existing workloads on some servers and deploying new applications and solutions on other servers.
- FusionCompute is the cloud OS software that virtualizes hardware resources and centrally manages virtual, service, and user resources. It also virtualizes compute, storage, and network resources. 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 and green data centers.
- FusionCompute Pro is a component for unified management of multiple resource sites in different regions. It uses virtual data centers (VDCs) to provide domain-based resource management capabilities for different users.

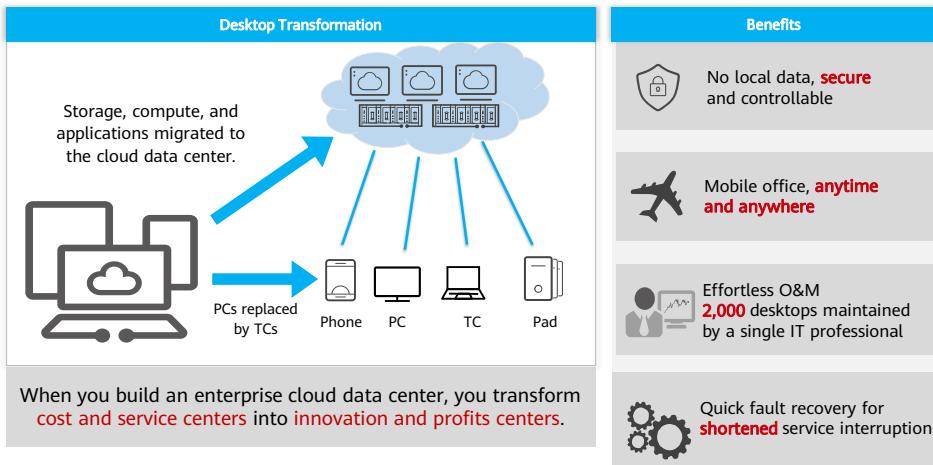
## Advantages of the FusionAccess (1)



- Data Stored in the Cloud for Enhanced Information Security
  - User data of conventional desktops, which is stored in local PCs, is prone to data breach or loss caused by cyber attacks. However, user data of virtual desktops is stored and processed on servers rather than on user terminals, preventing data breach or loss. In addition, security mechanisms such as TC access authentication and encrypted data transmission are employed to ensure the security and reliability of virtual desktops.
- Efficient Maintenance and Automatic Control
  - Conventional PC desktops are failure-prone. 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.
  - FusionAccess provides the powerful one-click maintenance tool to simplify the maintenance, allowing one IT professional to manage and maintain more than 2,000 virtual desktops in a centralized manner. Resource usage is automatically monitored to ensure load balancing among physical servers.
- Services Running in the Cloud for Higher Reliability
  - In conventional PC desktops, all services and applications run on local PCs, with 99.5% availability. However, with virtual desktops, all services and applications run in cloud data centers, delivering 99.9% reliability and reducing the management and maintenance costs.

- Mobile Office Enabled by Seamless Application Switchover
  - In the conventional desktop environment, users can access their personalized desktops only by using a single dedicated device. With virtual desktops, users can easily access their personal computer desktops.
- Reduced Noise and Power Consumption
  - Energy-saving and noise-free TCs reduce office noise from 50 dB to 10 dB. The total power consumption of a TC and liquid crystal display (LCD) is about 60 W, generating 70% lower electricity costs than a conventional PC. Reduced power consumption also means lower temperature control costs.
- Resource Elasticity and Sharing
  - All resources are stored in data centers to implement the centralized management and elastic scheduling, improving resource utilization. The average CPU utilization of conventional PCs is 5% to 20%. With virtual desktops, the CPU utilization of cloud data centers is about 60%, dramatically improving resource utilization.

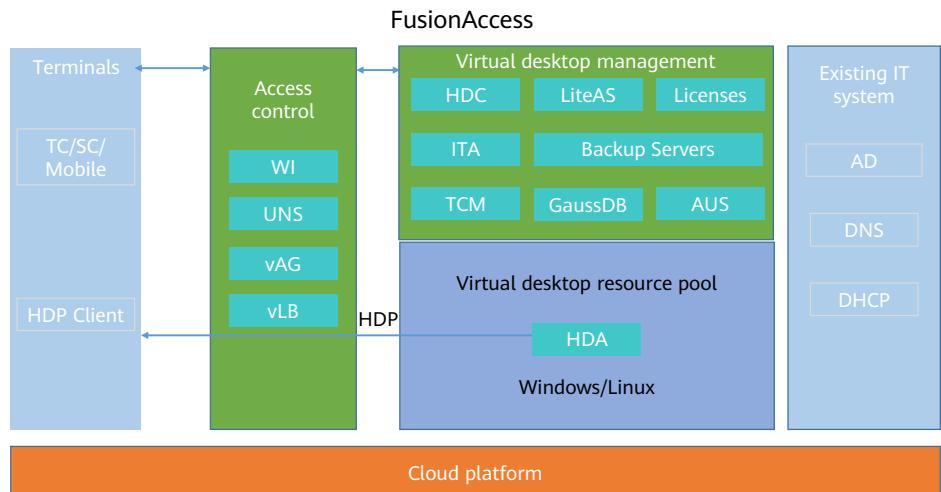
## Advantages of FusionAccess (2)



# Contents

1. Overview of FusionAccess
- 2. Introduction to FusionAccess Components**
3. Introduction to HDP
4. Introduction to FusionAccess Application Scenarios

## FusionAccess Overview



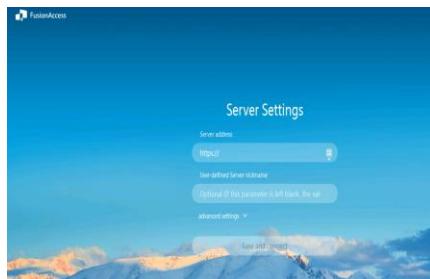
16 Huawei Confidential



- HDP Client: Installed on terminals that access virtual desktops.
- Huawei Desktop Agent (HDA): Installed on VMs and enables VMs 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.

## Access Control Layer (1)

- Web Interface (WI)
  - The WI provides a login page. After a user initiates a login request, the WI forwards the user login information (the encrypted username and password) to the active directory (AD) for authentication. If the authentication succeeds, the WI displays a computer list provided by the Huawei Desktop Controller (HDC). The user can then log in to any computer in the list.

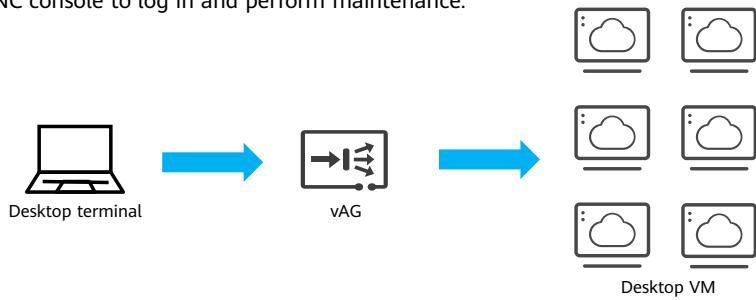


- Users can connect to, start, and restart VMs on the WI.

## Access Control Layer (2)

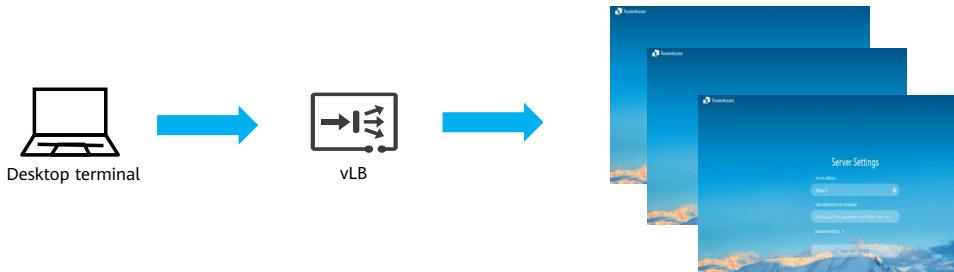
- Virtual Access Gateway (vAG)

- The vAG functions as a desktop access gateway and self-service console gateway. If a user's computer is faulty, and cannot be logged in to using a desktop protocol, the user can still use the VNC console to log in and perform maintenance.



## Access Control Layer (3)

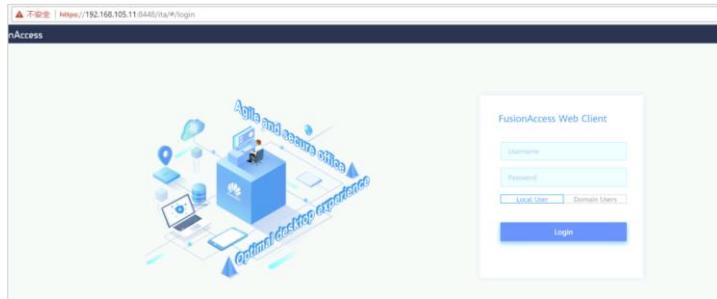
- Virtual Load Balancer (vLB)
  - The vLB performs load balancing to prevent too many users from accessing the same WI.



- 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.

## Virtual Desktop Management Layer (1)

- IT Adapter (ITA)
  - The ITA provides interfaces for users to manage VMs. It interacts with the HDC and the FusionCompute cloud platform software to create and assign VMs, manage VM statuses and templates, and operate and maintain VMs.



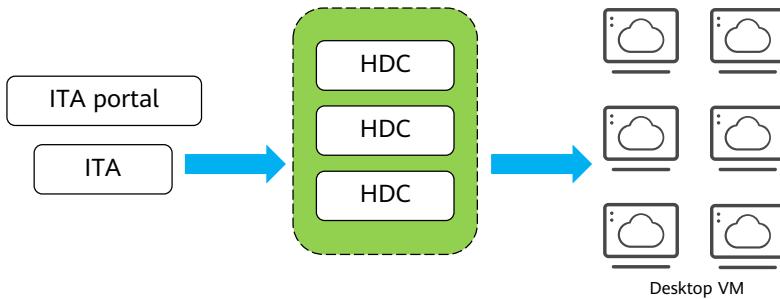
20      Huawei Confidential



- VMs are created, provisioned, and maintained on the ITA portal. The ITA calls the interface provided by the HDC.
- The ITA is a Tomcat-based Web service. Specifically, the ITA provides unified interfaces for the IT portal and interfaces for the HDC, FusionCompute, VMs, and DNSs.

## Virtual Desktop Management Layer (2)

- Huawei Desktop Controller (HDC)
  - The HDC is a core component for virtual desktop management. It manages desktop groups and assigns or unassigns VMs to or from users at the request of the ITA, and also processes VM login requests.



- One HDC can manage up to 5,000 desktops. One ITA can manage multiple HDCs and a maximum of 20,000 desktops. The HDC:
  - Implements and maintains the mapping between users and virtual desktops.
  - Exchanges access information with the WI and helps users access desktops.
  - Exchanges information with the HDA in the VM and collects information about the VM operating status and access status reported by the HDA.

## Virtual Desktop Management Layer (3)

- Thin Client Management (TCM)
  - The Cinfin Desktop Management System (CDMS) is used by administrator for TCM.

The screenshot shows the 'Client Group' section on the left with a tree view of groups like 'All Groups', 'Ungrouped Computers', and 'Inactive Computers'. On the right, the 'Client Information' table lists clients with columns: Alias, Parent group ..., IP, Agent Version, and System V... . The table contains five entries:

Alias	Parent group ...	IP	Agent Version	System V...
OEM-XFN0BXCN2D	All Groups	192.168.45.114	5.2.000.000.43045	3.33.05
WIN-HG08IU71AUJF	Inactive Com...	192.168.45.216	5.2.000.000.43045	3.38.05
OEM-MPLPBV0F49M	Inactive Com...	192.168.45.240	5.2.000.000.43045	3.33.05
WIN-S00GITSD1VA	Inactive Com...	192.168.98.65	5.2.000.000.43045	3.38.05



 HUAWEI

22      Huawei Confidential

- A management server provides centralized management for TCs, including version upgrade, status management, information monitoring, and log management.
- The management server can detect TCs to be managed and manage them in advance.

## Virtual Desktop Management (4)

- License Server
  - The License server manages and distributes licenses for the HDC.
  - FusionAccess uses the license for HDP connections. When a user attempts to connect to a VM, FusionAccess checks the license on the license server to determine whether the user can connect to the VM.

License Na...	IP Address	ESN	Software ID	Control Item	License Detail...	Expiry Date	Status
License	192.168.105.11	57C674D1732...		Desktop Count	Trial Edition(...)		Valid

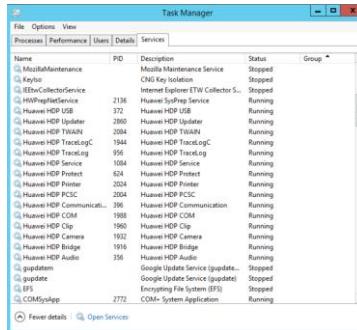
- The access licenses of FusionAccess are controlled by the license server.
- The total number of licenses is the number of purchased licenses. When the number of used licenses reaches 1.1 times the total number of licenses, new users cannot log in to the desktops.

## Virtual Desktop Management (5)

- GaussDB
  - GaussDB stores data for the ITA and HDC.
- BackupServer
  - The BackupServer is used to back up important files and data of components.
  - BackupServer backup policy:
    - The backup operation is performed at 01:00 a.m. every day and the backups are uploaded to `/var/ftpsite/<ITA name>/<folder of a component>` on the BackupServer.
    - The Backup Server retains backup data for 10 days. If backup space is insufficient, the system automatically deletes backups on a first-in first-out basis.

## Core Component of the Desktop VM - HDA

- Huawei Desktop Agent (HDA): installed on the virtual desktop to connect terminals.
- Thin client/Software client (TC/SC): According to the HDP protocol, a TC or SC can be connected to a VM only when the VM is configured with an HDA.
- HDA provides services for TCs or SCs to use VMs.



# Contents

1. Overview of FusionAccess
2. Introduction to FusionAccess Components
- 3. Introduction to HDP**
4. Introduction to FusionAccess Application Scenarios

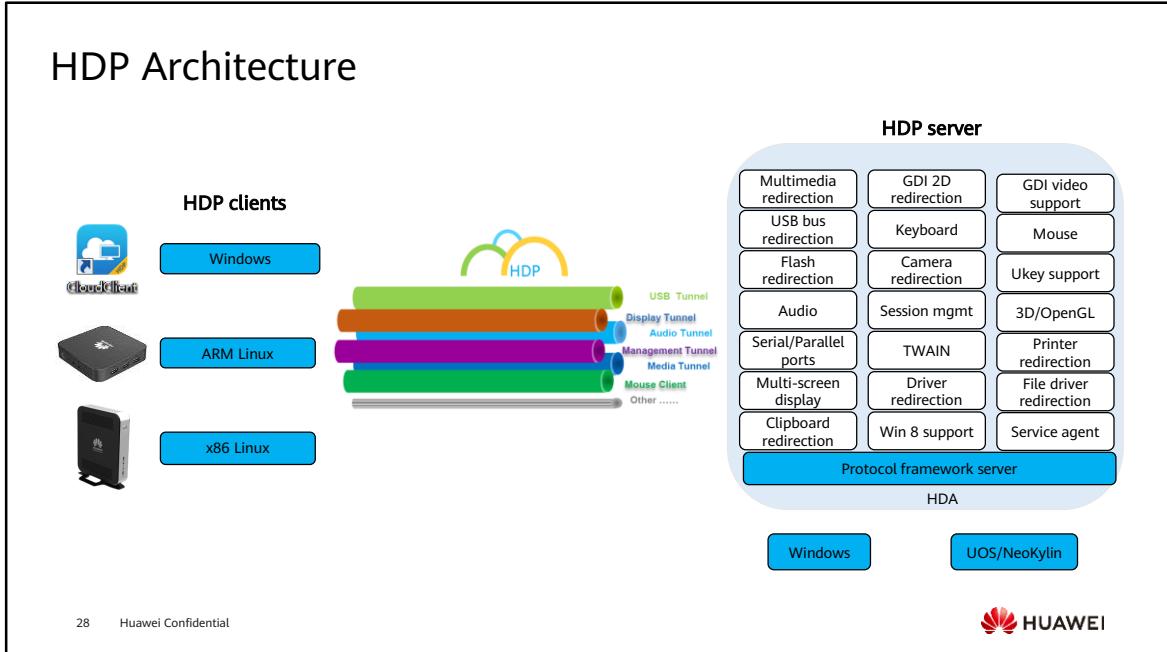
- As mentioned in the previous slides, the third platform built on cloud computing, computers, and virtualization has become the mainstream of the IT industry. Before we get into cloud computing, let's take a quick look at the evolution of computers and virtualization.

## 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



28      Huawei Confidential



- Windows desktops can only run on the x86 architecture.
- ARM-based Linux desktops are supported.

## 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 appropriate 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.

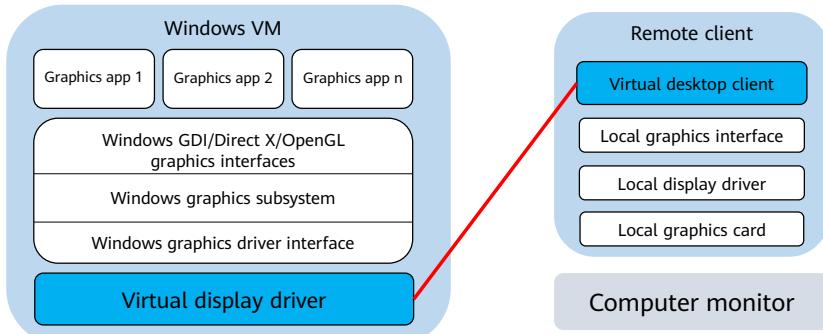
- In RDP, any authorized terminal can be a terminal server. Client can log in to the server and use the corresponding resources (including software and hardware). After the protocol is upgraded, client can even use the local resources (including the printer, audio playback, disks, and hardware interfaces). 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.



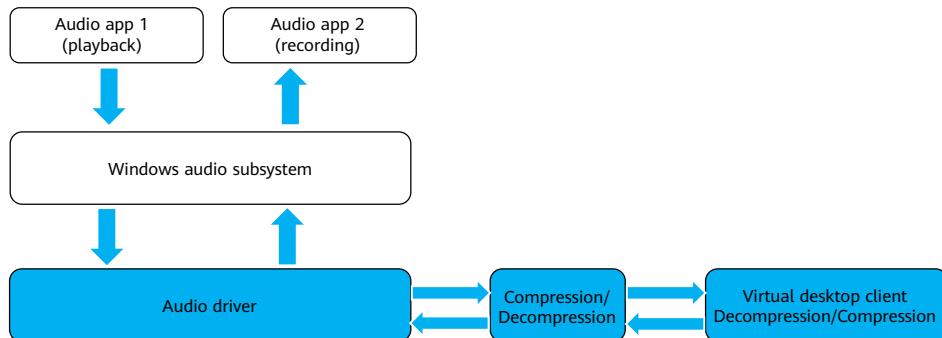
- As shown in the figure, in OS software layers, the display driver interacts with the graphics card. The upper-layer systems need to use the display driver to interact with the graphics card. Screen captures are transferred from the display driver to the graphics card of the remote TC to implement remote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



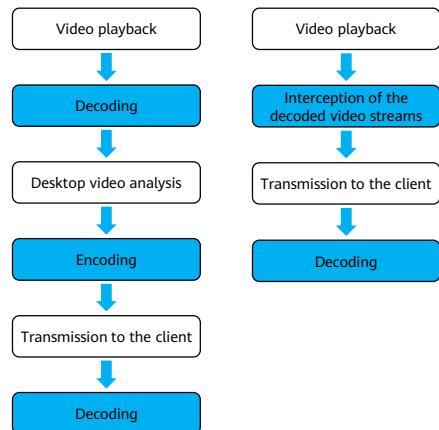
- During audio playback, the audio driver transmits audio data received from the Windows audio subsystem to the desktop protocol client after compression, and the client plays the audio after decoding. During audio recording, the client transmits local recording data to the server after compression, 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)

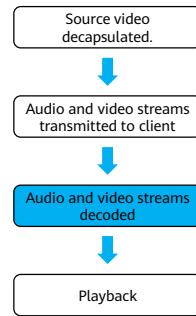
- Currently, Huawei Desktop Protocol supports two types of video playback:
  - Video recoding: Multimedia playing on the server is re-coded before being transmitted to the client for decoding and display.
  - Video redirection: Video streams on the server are captured and transmitted directly to the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



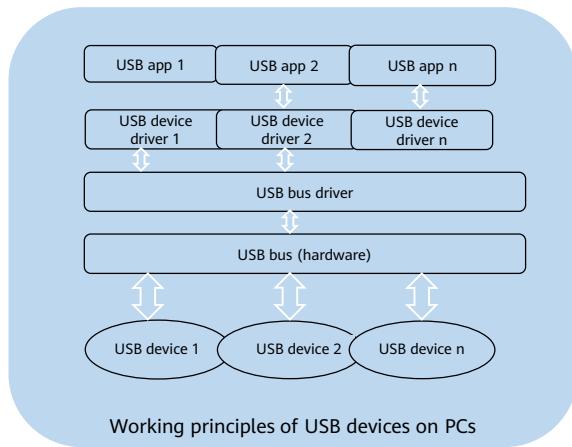
## HDP - Display Technology (3)

- 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)

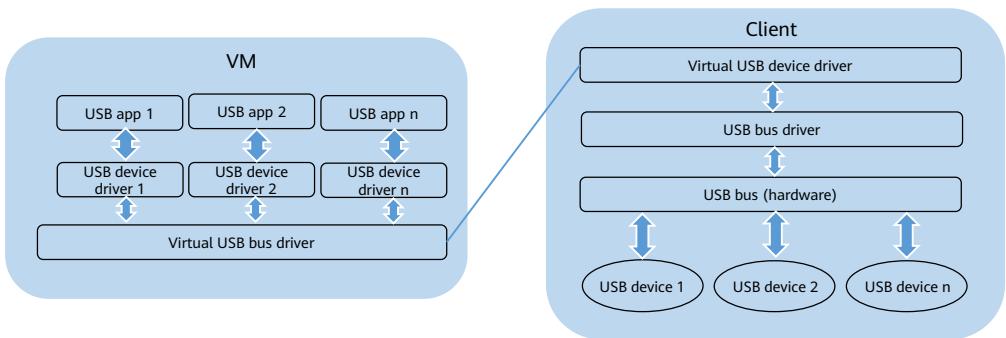
- In virtual desktops, peripherals on the TC/SC side are mapped to a remote desktop using desktop protocols. Depending on how they are used, peripheral technologies are classified as either port redirection or device redirection:
  - Port redirection: The port protocols are redirected to the OSs of the 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)



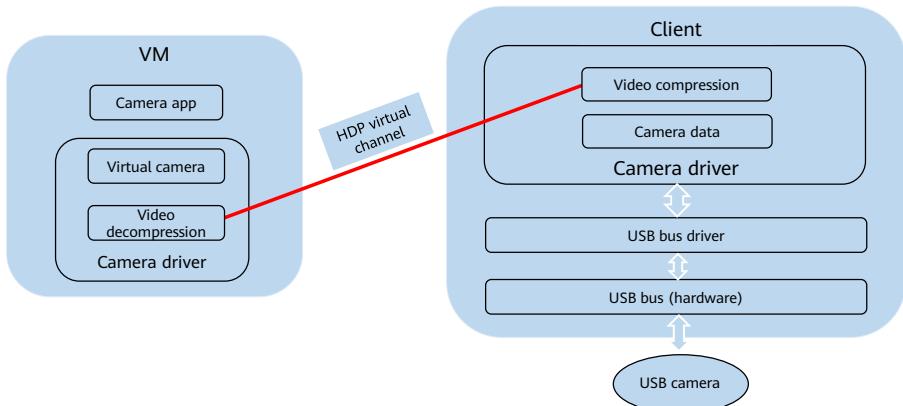
- The preceding figure shows that the USB bus driver is essential for enabling USB devices to work normally at the software layer. When an application needs to use a USB peripheral, it must interact with the USB device driver. The USB device driver relies on the USB bus driver to exchange data with the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

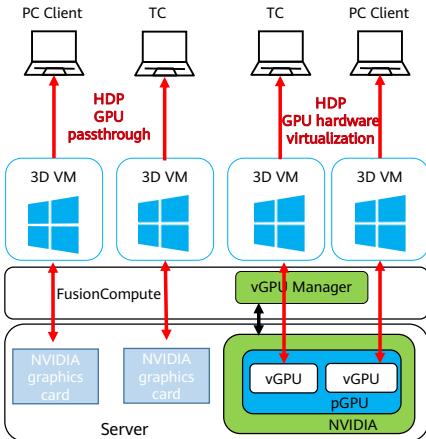
## HDP - Peripheral Redirection (4)



- 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



45      Huawei Confidential



- 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

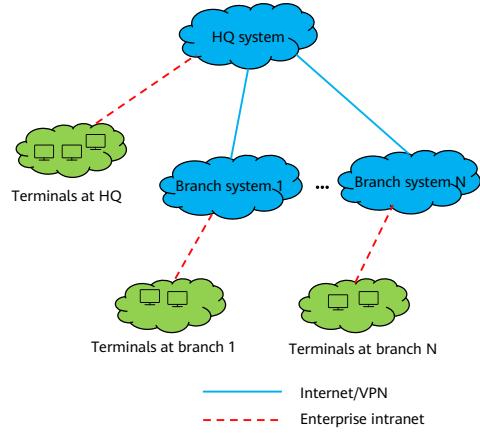
1. Overview of FusionAccess
2. Introduction to FusionAccess Components
3. Introduction to HDP
- 4. Introduction to FusionAccess Application Scenarios**

## FusionAccess Application Scenarios



## 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

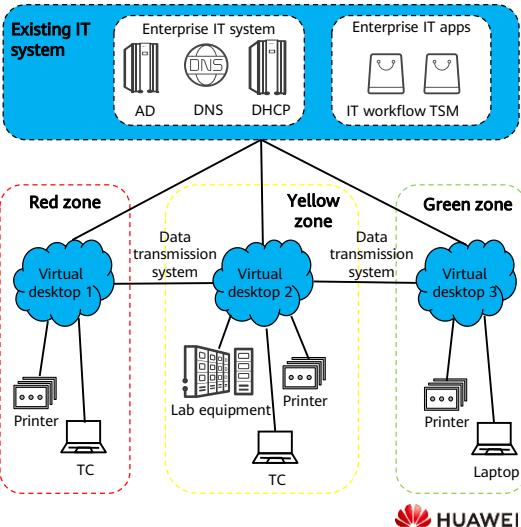
- Introduction

- 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

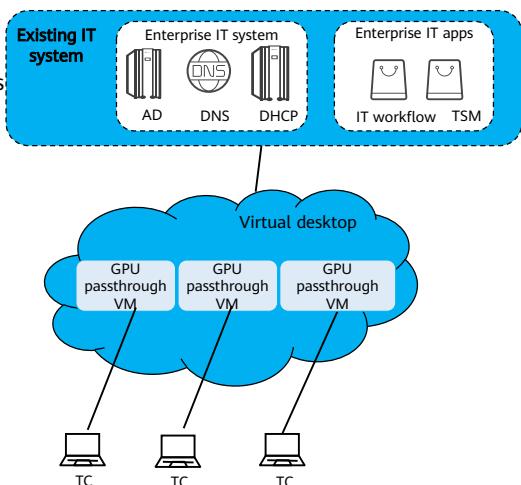
49      Huawei Confidential



- 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 and animation rendering.
- Benefits
  - Reused physical GPU resources
  - Reduced costs
  - Centralized data management



50      Huawei Confidential



- 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.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



## 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.

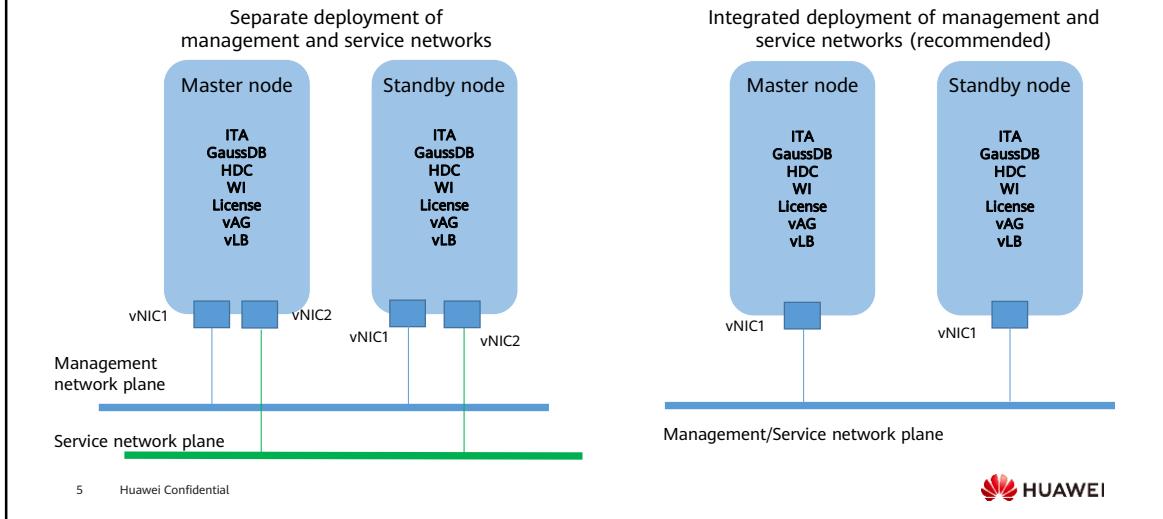
# Objectives

- Upon completion of this course, you will understand:
  - Installation of basic Linux components
  - Functions and basic features of Windows AD
  - Installation and configuration of the AD, DNS, and DHCP
  - FusionAccess initial configuration

# Contents

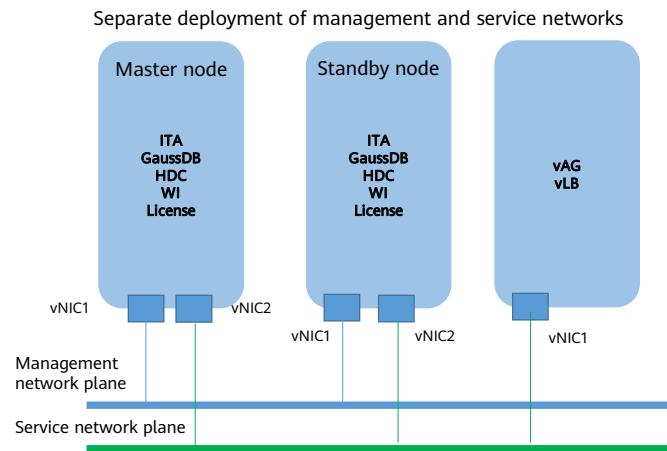
- 1. FusionAccess Component Planning and Deployment**
  - FusionAccess Management Component Installation Planning
  - FusionAccess-associated Components
  - FusionAccess-associated Component Installation Planning
2. FusionAccess Installation
3. FusionAccess Initial Configuration

## FusionAccess Component Installation Planning: Integrated Deployment



- The active and standby VMs must be deployed on different CNA nodes.
- Port group:
  - Port group for the management plane NICs of FusionAccess 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 FusionAccess infrastructure VMs: 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 the **ManagementDVS**. 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.
- All components can be installed on one VM or different VMs. For example, the ITA, GaussDB, HDC, WI, and License components can be installed on one VM, and the vAG and vLB components can be installed on another VM. In a commercial environment, only one component is deployed on a VM to improve performance.

## FusionAccess Component Installation Planning: Standard Deployment (1)

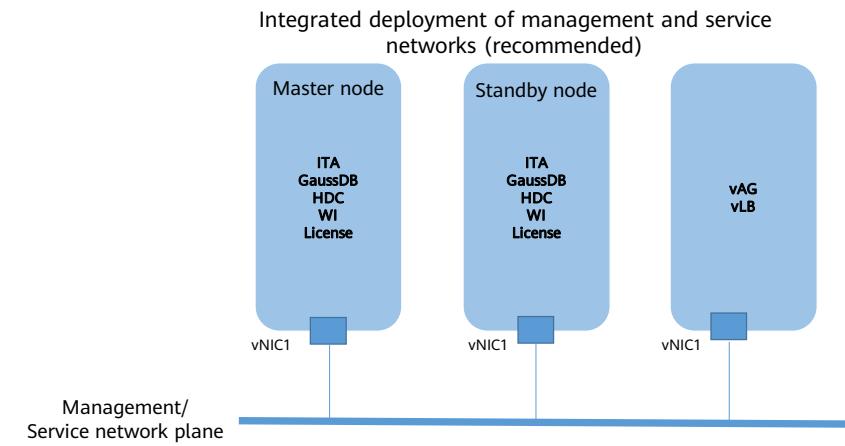


6      Huawei Confidential



- The active and standby VMs must be deployed on different CNA nodes.

## FusionAccess Component Installation Planning: Standard Deployment (2)



- The active and standby VMs must be deployed on different CNA nodes.

## FusionAccess Component Installation Planning (3)

Mode	VM	Deployment	OS	Hardware Specification	NIC
Integrated deployment	Linux infrastructure VM	Active/standby	Select <b>EulerOS 2.8 64 bit</b> for Arm architecture. Select <b>EulerOS 2.5 64 bit</b> for x86 architecture.	CPU: 8 cores Memory: 16 GB Disk: 60 GB	vNIC1: service plane vNIC2: management plane
Standard deployment	ITA/GaussDB/HDC/WI/License/LiteAS	Active/standby	Select <b>EulerOS 2.8 64 bit</b> for Arm architecture. Select <b>EulerOS 2.5 64 bit</b> for x86 architecture.	CPU: 8 cores Memory: 16 GB Disk: 60 GB	vNIC1: service plane vNIC2: management plane
	vAG	Multi-active	Select <b>EulerOS 2.8 64 bit</b> for Arm architecture. Select <b>EulerOS 2.5 64 bit</b> for x86 architecture.	CPU: 4 cores Memory: 4 GB Disk: 40 GB	vNIC1: service plane
	vLB	Active/standby	Select <b>EulerOS 2.8 64 bit</b> for Arm architecture. Select <b>EulerOS 2.5 64 bit</b> for x86 architecture.	CPU: 8 cores Memory: 4 GB Disk: 40 GB	vNIC1: service plane

- Optional Linux infrastructure VMs include:
  - Backup Server
  - TCM: Thin Client Manager
- Components can be installed on one VM or different VMs. The installation planning depends on the actual networking and requirements.

# Contents

- 1. FusionAccess Component Planning and Deployment**
  - FusionAccess Management Component Installation Planning
  - **FusionAccess-associated Components**
    - FusionAccess-associated Component Installation Planning
2. FusionAccess Installation
3. FusionAccess Initial Configuration

# 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.

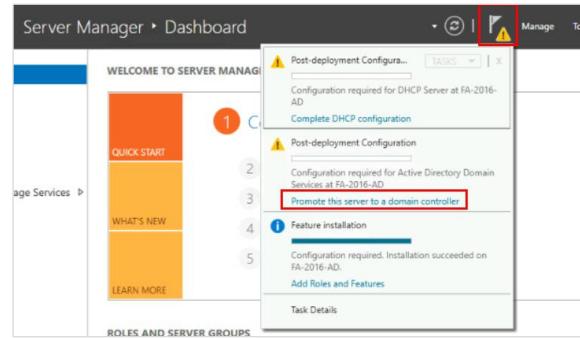
- AD is a sophisticated service component for Windows Server OS. AD processes network objects, including users, groups, computers, network domain controllers, emails, organizational units, and trees in organizations.
- The AD provides the following functions:
  - Basic network services, including DNS, 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.

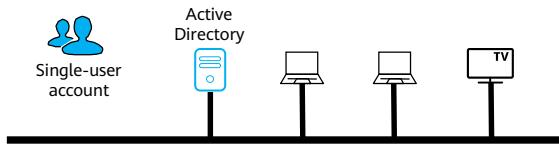
## Domain Controller

- 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.



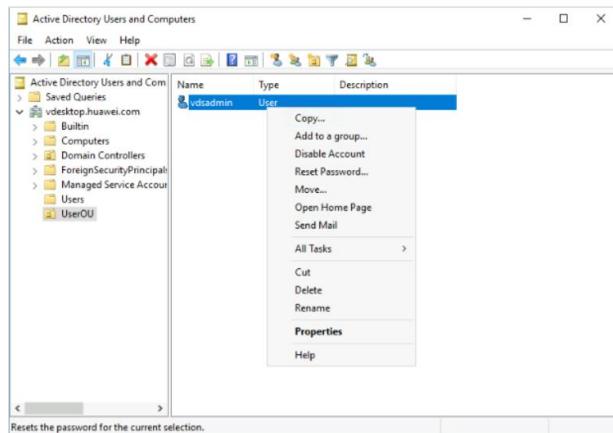
## Domain User Account

- 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.

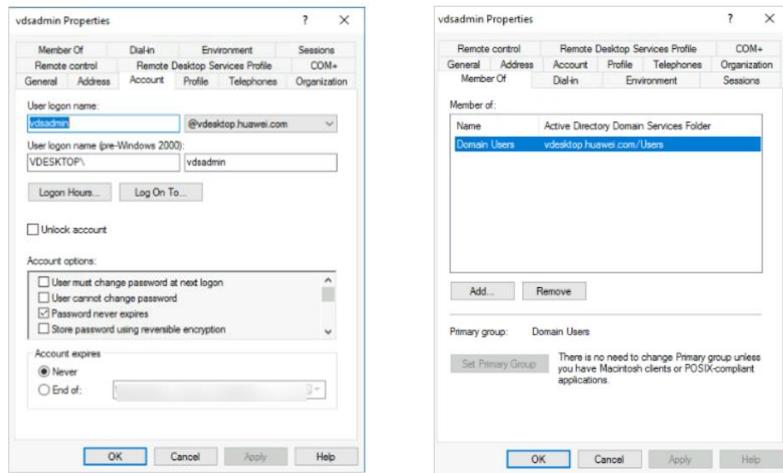


## Common Operations on Domain Accounts

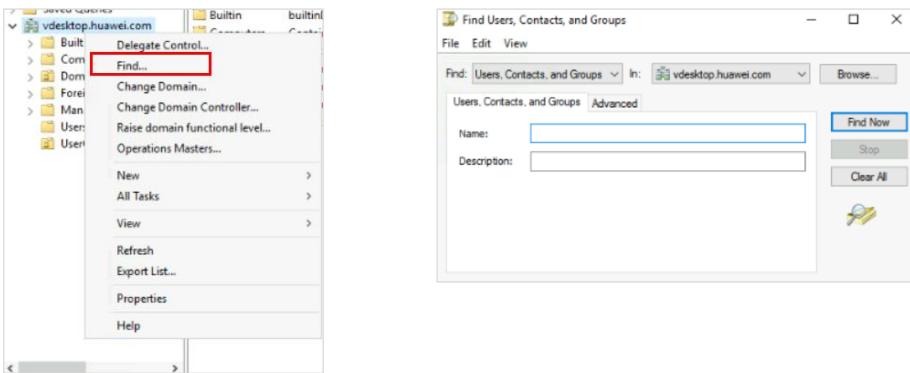
- Add to group
- Disable account
- Reset password
- Move
- Delete
- Rename



## User Domain Account Properties

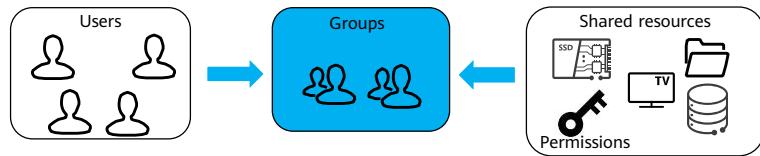


## Finding a User Domain Account



## User Group

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



## Groups in the AD

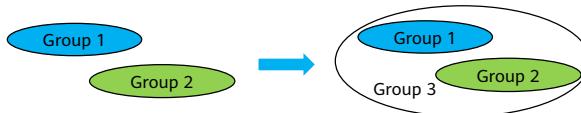
- Groups simplify the allocation of resource permissions.



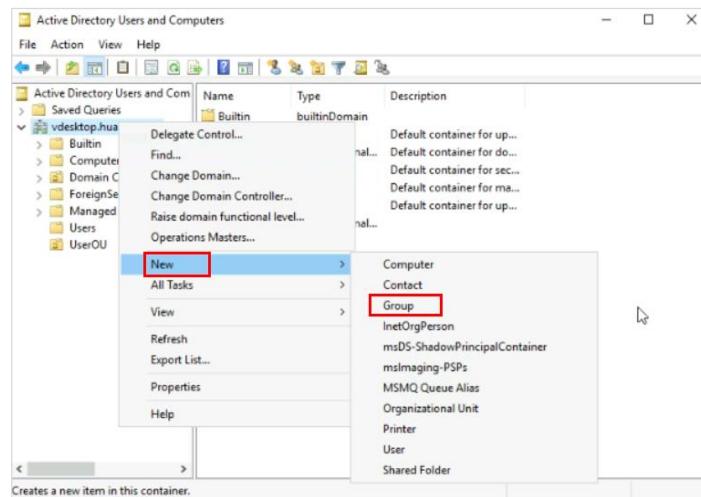
- A user can join multiple groups.



- A group can be nested in another group.

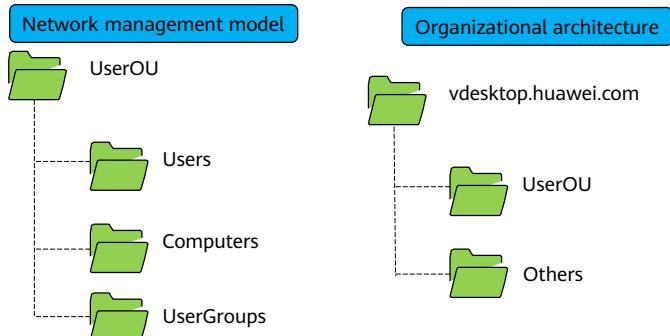


## Creating a User Group

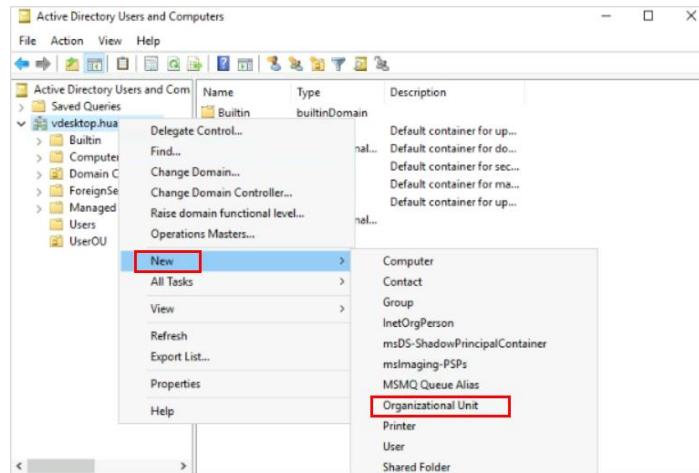


## Organization Unit (OU)

- 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.



## Creating an OU

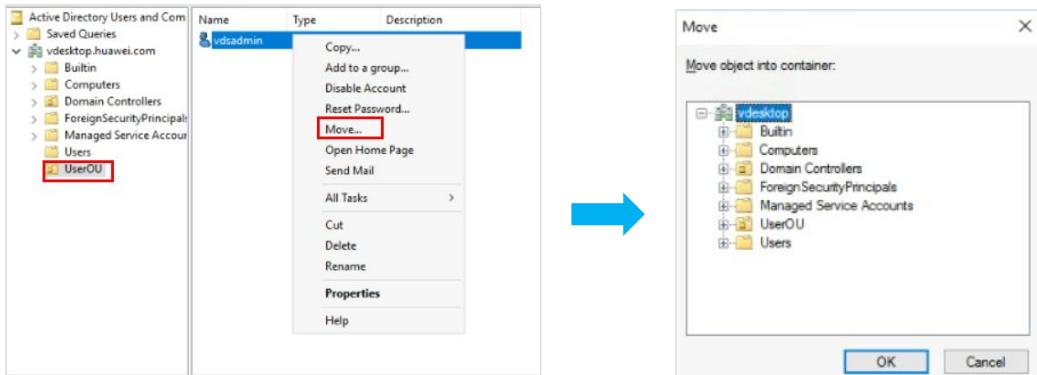


21 Huawei Confidential



- 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.

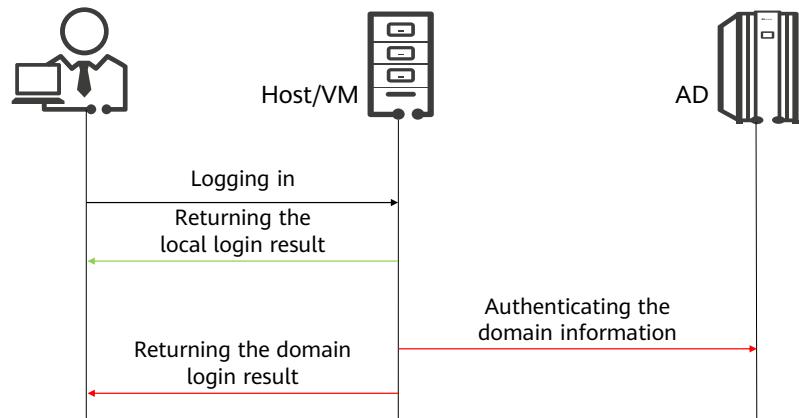
## User Groups vs. OUs

- 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.

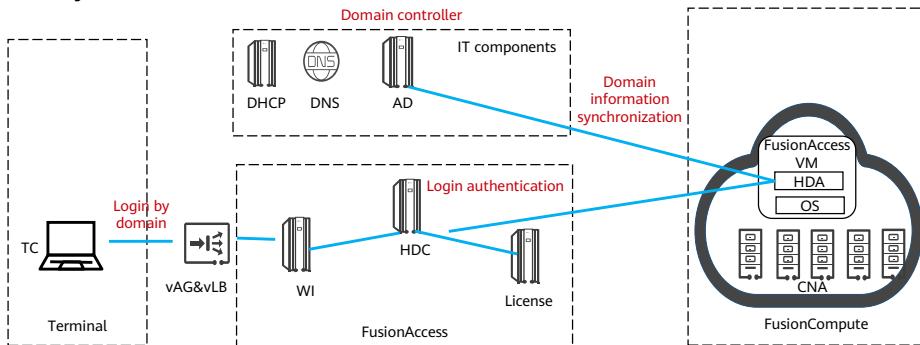
## Adding a Computer to an AD Domain



- 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.



## Domain Name System (DNS)

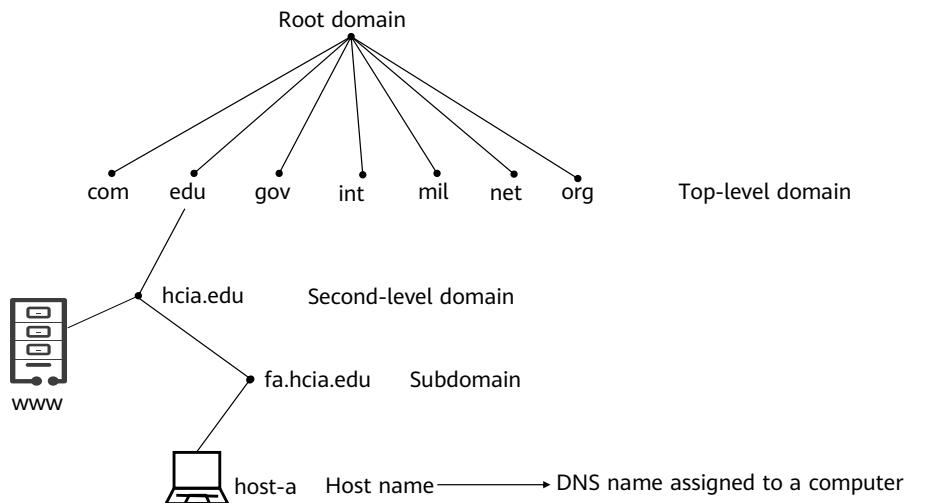
- DNS is a distributed database that converts IP addresses and domain names for network access.
- DNS advantages:
  - Users can access the network with easy-to-remember character strings, instead of IP numbers.
  - DNS cooperates with the domain controller.
  - A domain controller registers its role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

## DNS Domain Name Structure (2)

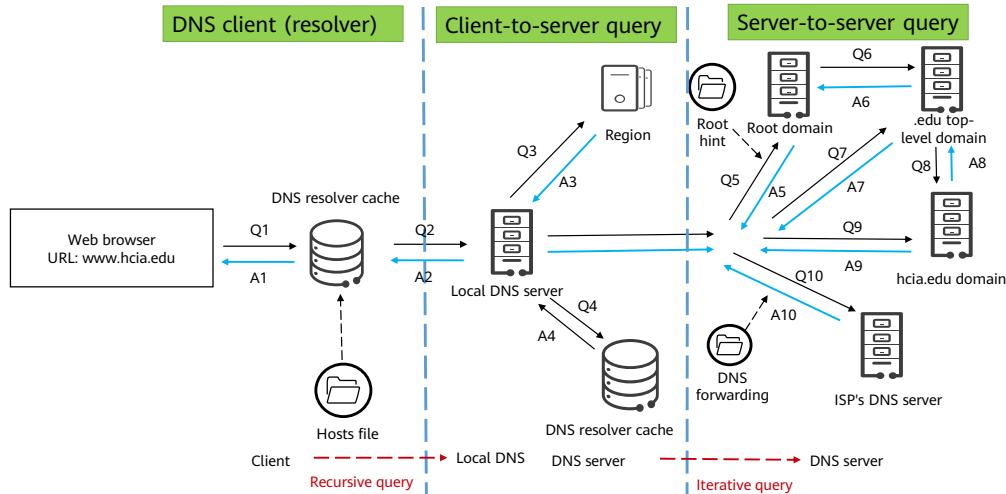


29      Huawei Confidential



- 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).

## How DNS Works



30      Huawei Confidential



- **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**.

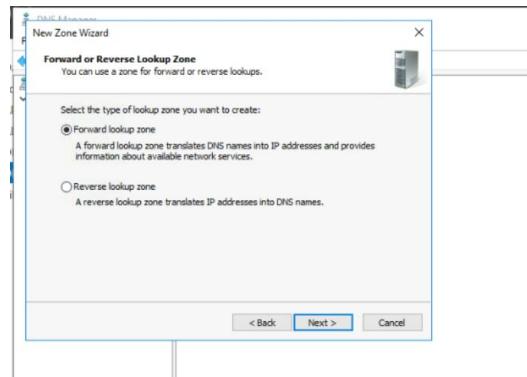
- The following shows three ways for the host of **www.abc.com** to query the IP address of the server of **www.xyz.abc.com**:

- 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.

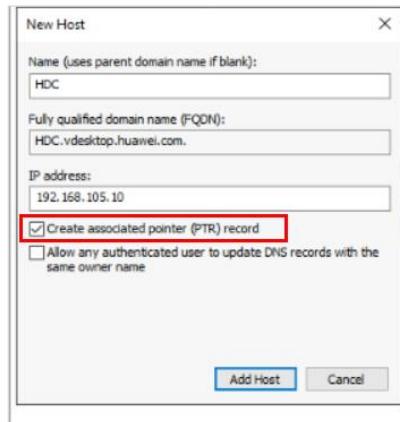
## DNS Forward Lookup

- 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.



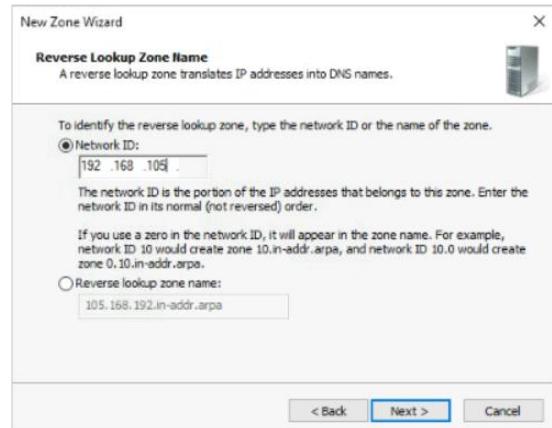
## Adding a DNS Record

- 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.



## 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.

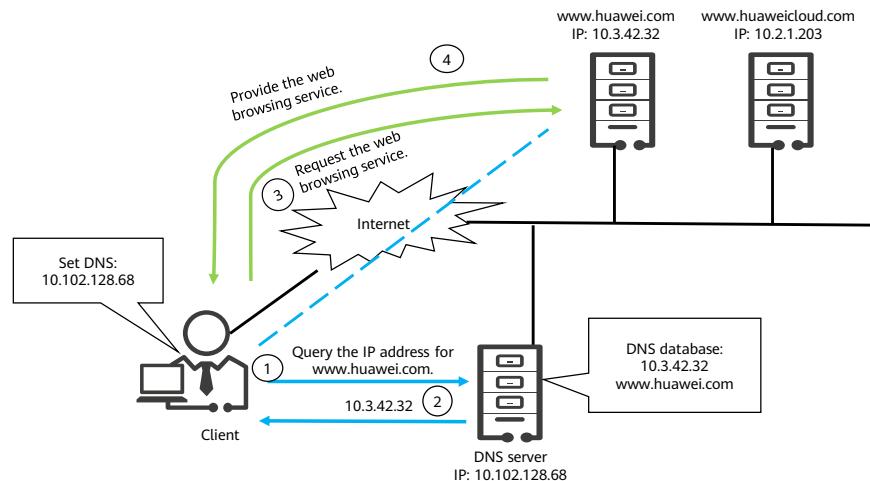
## Client DNS Configuration

- Configure the DNS server address for clients.



 HUAWEI

## DNS Working Process



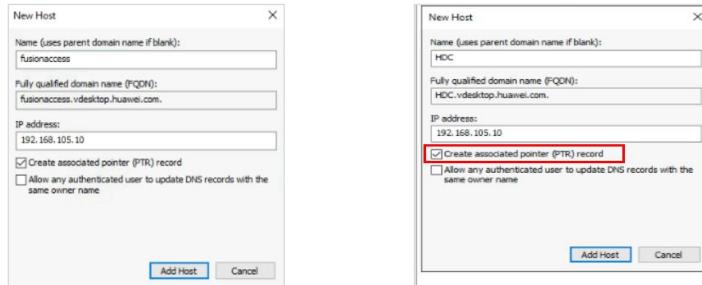
37      Huawei Confidential



- 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.

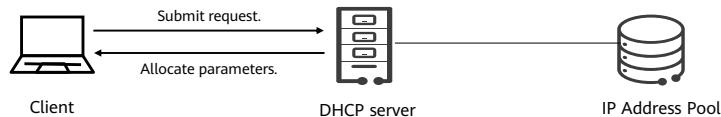
## DNS Resolution in FusionAccess

- 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.



## DHCP

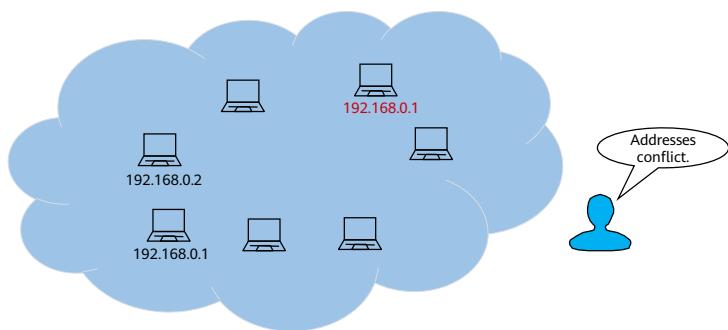
- DHCP is a communication protocol for network administrators to centrally manage and automatically assign IP addresses.
- After receiving a client request, the DHCP server provides the terminal with parameters (IP address, default gateway, and DNS server IP address).



- 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)

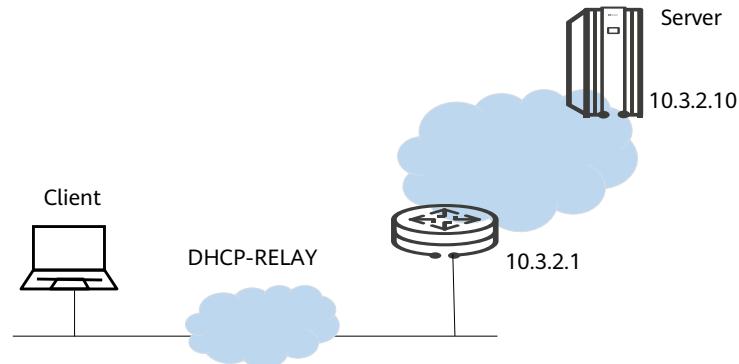
- In a TCP/IP network, each workstation must perform basic network configurations before accessing the network and its resources. Mandatory parameters include the IP address, subnet mask, default gateway, and DNS. Required information includes IP management policies.
- In larger networks, it is difficult 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

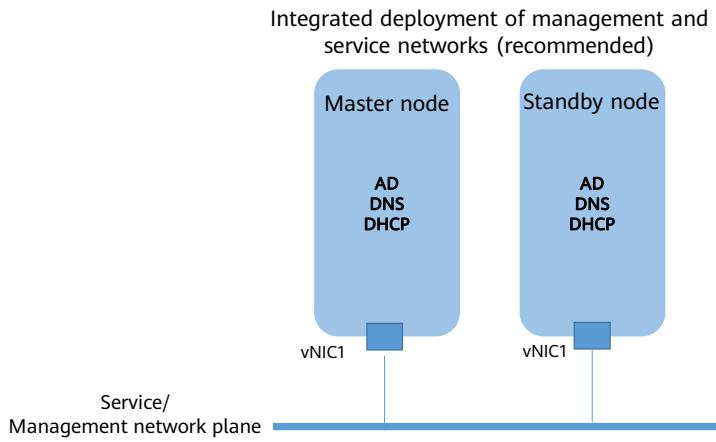


- If a DHCP server configures the network for the computers on another network, you can configure a DHCP-RELAY to process and forward DHCP information between different subnets and physical network segments.

# Contents

- 1. FusionAccess Component Planning and Deployment**
  - FusionAccess Management Component Installation Planning
  - FusionAccess-associated Components
    - FusionAccess-associated Component Installation Planning
2. FusionAccess Installation
3. FusionAccess Initial Configuration

## FusionAccess-associated Component Installation Planning (1)



- The active and standby VMs must be deployed on different CNA nodes.

## FusionAccess-associated Component Installation Planning (2)

VM	Deployment	OS	Hardware Specification	NIC
AD/DHCP/DNS	Active/standby	Windows Server 2016 R2 Standard 64 bit	CPU: 2 cores Memory: 2 GB Disk 1: 50 GB (system disk) Disk 2: 20 GB (backup disk)	vNIC1: service plane

- The AD is an information database that stores information such as accounts, passwords, and organizations.

# Contents

1. FusionAccess Component Planning and Deployment
- 2. FusionAccess Installation**
3. FusionAccess Initial Configuration

## Management Component Installation

- Configure the cloud platform.
- Create a Linux infrastructure VM.
- Install the ITA/GaussDB/HDC/WI/License.
- (Optional) Install the vAG/vLB.

# Configuring the Cloud Platform

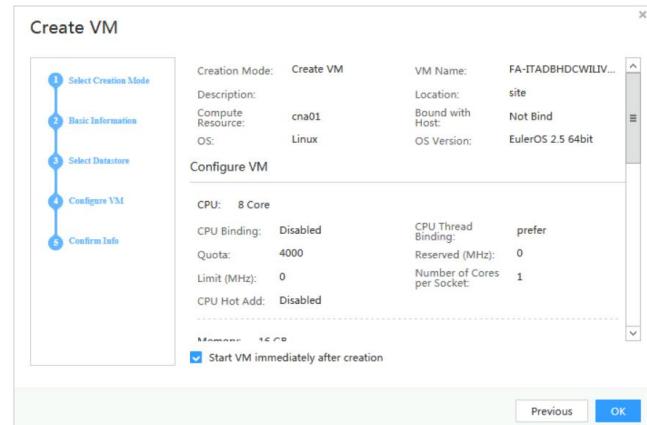
- Configure the network.
  - Create DVSs.
  - Create port groups.
- Configure data storage.
  - Associate with storage resources.
  - Allocate storage devices and map them to clusters.
  - Create datastores.

The screenshot displays three main configuration sections:

- Resource Pools > Network**: Shows a table for creating DVSs. A row for "ManagementDVS" is selected, highlighted with a red box. The table includes columns for Name, Switch Type, Port Groups, Jumbo Frames, and IGMP Snooping.
- Resource Pools > Port Group**: Shows a table for managing port groups. A row for "managePortgroup" is selected, highlighted with a red box. The table includes columns for Name, Type, Connection Method, VLAN, and Description.
- Resource Pools > Storage**: Shows a table for managing datastores. Two entries are listed: "autoDS\_cna01" and "autoDS\_cna02". Both are highlighted with red boxes. The table includes columns for Name, Status, Type, Total Capacity, Allocated Capacity, and Available Capacity.

## Creating a Linux Infrastructure VM (1)

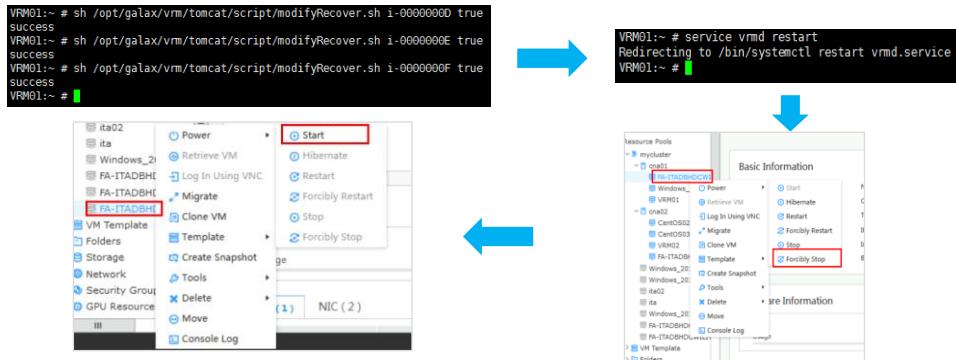
- Create a Linux infrastructure VM as planned.



## Creating a Linux Infrastructure VM (2)

- Configuring Linux Infrastructure VMs

- Enable automatic recovery.



51      Huawei Confidential



- After the VRM process is restarted, log in to FusionCompute again to power off and on the VM.

## Creating a Linux Infrastructure VM (3)

- Install the VM OS from the virtual drive, restart and log in to the VM, and configure the IP address, subnet mask, and gateway of the VM as planned.



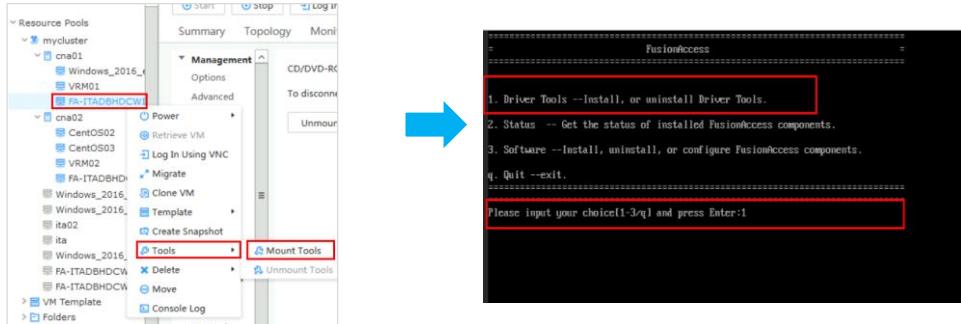
```
Authorized users only. All activities may be monitored and reported.  
FusionAccess#1 login: root  
Password:  
Authorized users only. All activities may be monitored and reported.  
Please input ip address and press Enter: 192.168.10.10  
Please input subnet mask and press Enter: 255.255.255.0  
Please input gateway and press Enter: 192.168.105.254
```

```
Authorized users only. All activities may be monitored and reported.  
FusionAccess#1 login: [root] Reached Target. MultiUser Started.  
[root] Starting Update UTP about System Baseline Changes...  
[root] [  ] I Started Update UTP about System Baseline Changes.  
[root] [  ] I Mounted /etc/ntp/ntp.conf File System.  
[root] [  ] I Mounted /etc/ntp/ntp.conf.d File System.  
[root] [  ] I Mounted /etc/ntp/ntp.conf.d.dhcp File System.  
[root] [  ] I Started Crash recovery kernel service.
```

- The built-in script of FusionAccess 8.0 infrastructure VM image is automatically installed. After the installation is complete, configure the VM as prompted.
- VNC login: Log in to the VM using VNC as the **root** user (preset password: **Cloud12#\$**).

## Creating a Linux Infrastructure VM (4)

- Mount Tools (Driver Tools) to the VM.



## Installing the ITA/GaussDB/HDC/WI/License/vAG/vLB (1)



54      Huawei Confidential



- The converged deployment of the ITA/GaussDB/HDC/WI/License/vAG/vLB/LiteAS components was introduced in the preceding slides.
- Node selection:
  - When installing an active component, select **Create a new node**.
  - When installing a standby component, select **Add to an existing node**.
- Installation mode, which should be the same as that of FusionCompute:
  - Common mode
  - Rights separation mode (High Security)

## Installing the ITA/GaussDB/HDC/WI/License/vAG/vLB (2)

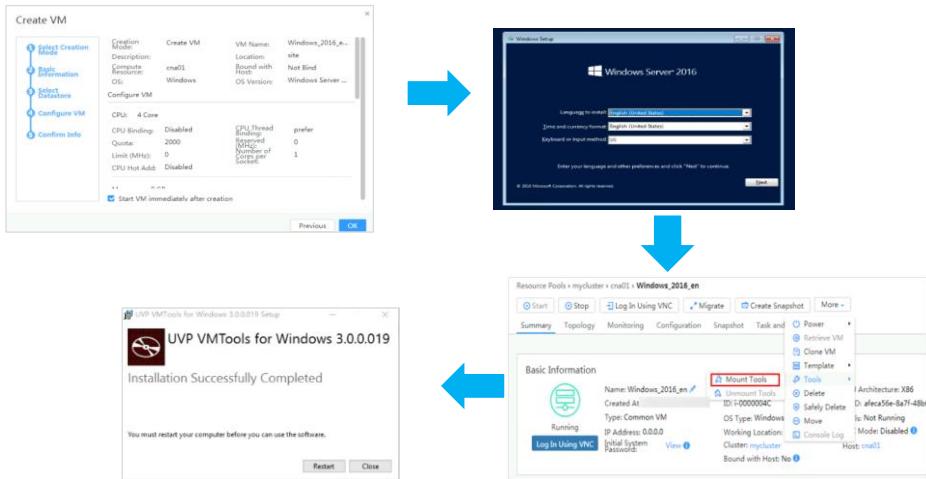
```
1. Common mode
2. Rights separation mode(High Security)
q. Back
=====
Please input your choice(1~2~q) and press Enter:1
You have chosen Common mode
Local Service IP:192.168.195.18
16:35:17[Info]:Begin to check FusionAccess component.
16:35:18[Info]:No FusionAccess component are already installed.
16:35:51[Info]:Begin to install ITA.
16:36:03[Info]:Begin to install WI.
16:36:28[Info]:Begin to install License.
16:36:39[Info]:Begin to install GaussDB.
16:37:01[Info]:Begin to install HDC.
16:37:29[Info]:Begin to install vLB.
16:37:49[Info]:Begin to install LiteS.
16:38:39[Info]:Begin to install Cache.
16:38:48[Info]:Configure LiteS name...
16:38:48[Info]:Configure LiteS successfully.
16:38:48[Info]:Start to config WIs to vLB...
16:39:01[Info]:Config WIs to vLB successfully.
16:39:01[Info]:Config ha to single mode...
16:39:01[Info]:Config ha to single mode successfully.
16:39:48[Info]:Restart ha...
16:39:48[Info]:Restart successfully.
16:39:04[Info]:Config Cache ...
16:39:04[Info]:Config Cache successfully.
16:39:04[Info]:Config HDC...
16:39:10[Info]:Config HDC successfully.
16:39:10[Info]:Config WI...
16:39:16[Info]:Config WI successfully.
16:39:16[Info]:Configure ITA...
```

- Specify the **Local Service IP** (the service plane IP address of the local server) and press **Enter**.
- The system starts installing and configuring components.
- After the message **Install all components successfully** is displayed, the components have been installed.

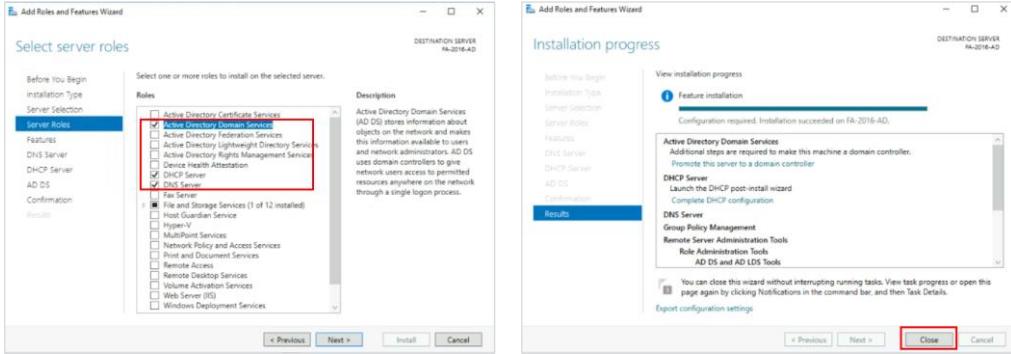
## FusionAccess-associated Component Installation

- Create a Windows infrastructure VM.
- Install the AD/DNS/DHCP component.
- Configure the AD service.
- Configure the DNS service.
- Configure the DHCP service.

# Creating a Windows Infrastructure VM

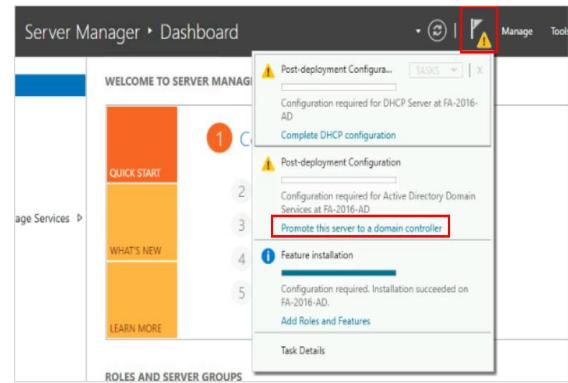


# Installing the AD Component



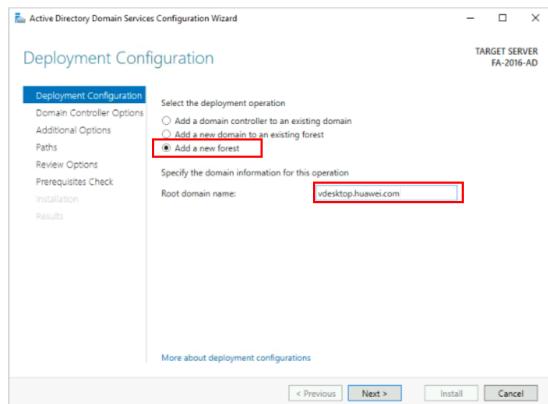
## Configuring the AD Service (1)

- Create a domain.
- Configure domain users and policies.



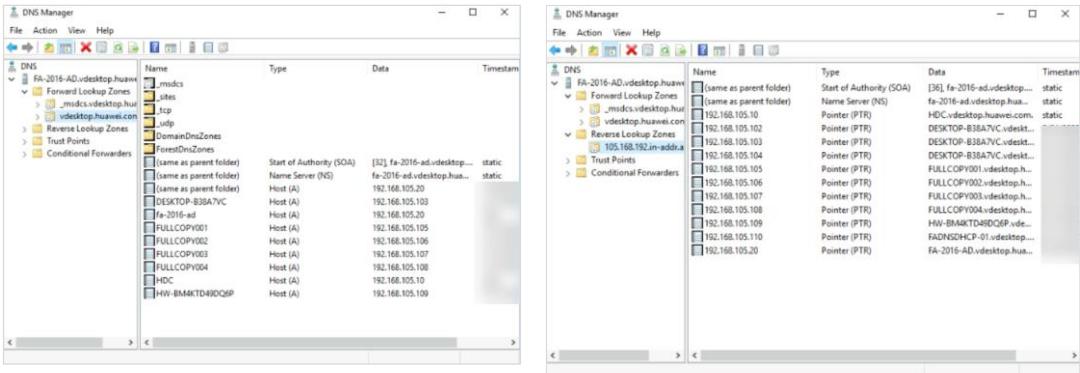
## Configuring the AD Service (2)

- Create a domain.
- Configure domain users and policies.



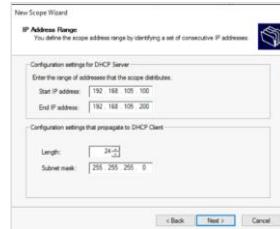
# Configuring the DNS Service

- Configure the DNS forward and reverse lookup function.



## Configuring the DHCP Service

- Configure the DHCP scope and related network parameters to distribute network configuration information to computers within the scope.
- These parameters are:
  - Range of IP addresses
  - Default gateway
  - Lease period
  - Domain name and DNS server



 HUAWEI

# Contents

1. FusionAccess Component Planning and Deployment
2. FusionAccess Installation
- 3. FusionAccess Initial Configuration**

## Modifying a Timestamp

- To prevent failures caused by asynchronous desktop provisioning, modify the configuration file and disable time verification after the installation.

```
192.168.105.10 - PuTTY
login as: gandalf
Authorized users only. All activities may be monitored and reported.
gandalf@192.168.105.10's password:
Last login:
Authorized users only. All activities may be monitored and reported.
[gandalf@fusionaccess01 ~]$ 
[gandalf@fusionaccess01 ~]$ 
[gandalf@fusionaccess01 ~]$ sudo su
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for gandalf:
Sorry, user gandalf is not allowed to execute '/bin/su' as root on fusionaccess01.
[~]$
[gandalf@fusionaccess01 ~]$ su - root
Password:
su: Permission denied
```

64      Huawei Confidential



- Log in to the active ITA/GaussDB/HDC/WI/License/vAG/vLB/LiteAS VM using PuTTY as the **gandalf** user.
- Run the following command to switch to the **root** user:
  - su - root**
  - Enter the **root** password (**Cloud12##** by default).
- Run the following command to modify **SystemConf.xml**:
  - Press **I** to enter editing mode and change the value of **HdaToHdcTimeCheck** to **0**.
  - <HdaToHdcTimeCheck>0</HdaToHdcTimeCheck>**
- Press **Esc** to exit editing mode. Enter **:wq** and press **Enter** to save the settings and exit.
- Run the following command to restart the ITA service:
  - service ITAService restart**

## Performing Initial Configuration

- After installing FusionAccess management and associated components, log in to the ITA portal to perform initial configuration.
  - Configure the virtualized environment.
  - Configure the vAG/vLB.
  - Configure a default policy.
  - Confirm the information.



- In the address box of your web browser, enter ***https://Service plane IP address of the active ITA VM:8448***, and press **Enter**.
  - Set the password for the **admin** user upon the first login.

## Configuring the Virtualized Environment

The screenshot shows a configuration interface for FusionAccess. At the top, there are three tabs: 'Configure a virtualized environment' (selected), 'Configure vAG/vLB', and 'Configure Default Policy'. Below the tabs, a message reads: 'Configure the virtualization environment for FusionAccess. The virtualization environment only can be FusionCompute currently.' There are several configuration fields:

- FusionCompute IP: Address -  (disabled)
- FusionCompute Port Number:  7070
- SSL Port Number:  7443
- Username:  vdisysman
- Password:
- Protocol:  http (unchecked)  https (checked)
- Description:

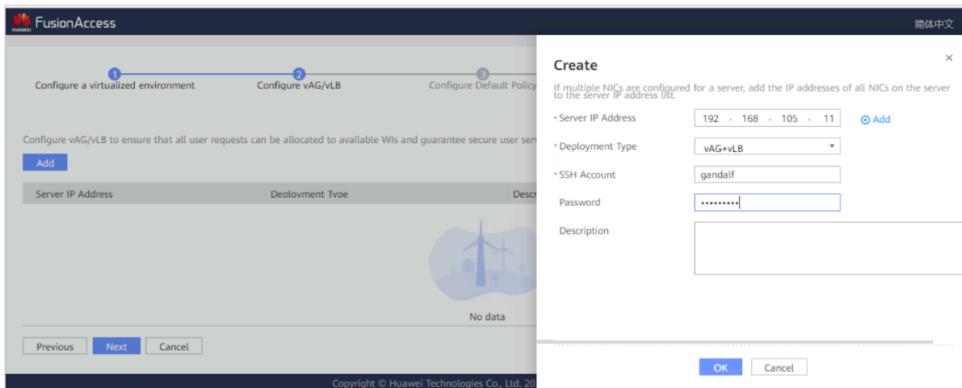
At the bottom are 'Next' and 'Cancel' buttons.

66      Huawei Confidential



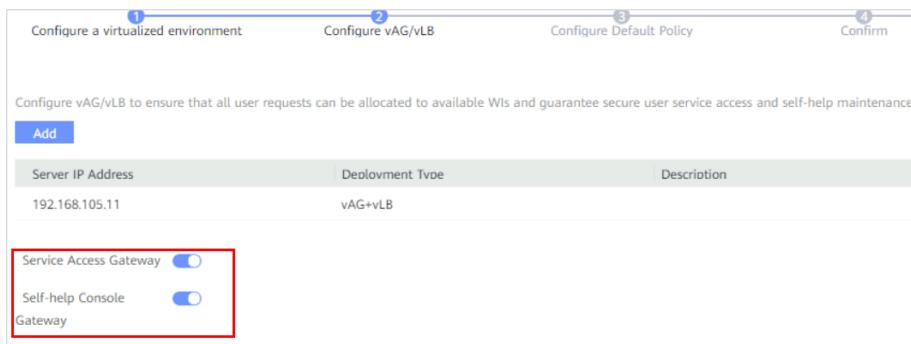
- **FusionCompute IP Address:** Enter the floating IP address of the Virtual Resource Management (VRM) node.
- **FusionCompute Port Number:** Enter **7070**.
- **SSL Port Number:** Enter **7443**.
- **Username:** The default value is **vdisysman**.
- **Password:** The default value is **VdiEnginE@234**.
- **Protocol:** Select the protocol used for communication between FusionCompute and the ITA. You are advised to select **https**.
  - If the communication protocol is set to **http**, you need to enable port 7070.

## Configuring the vAG/vLB (1)



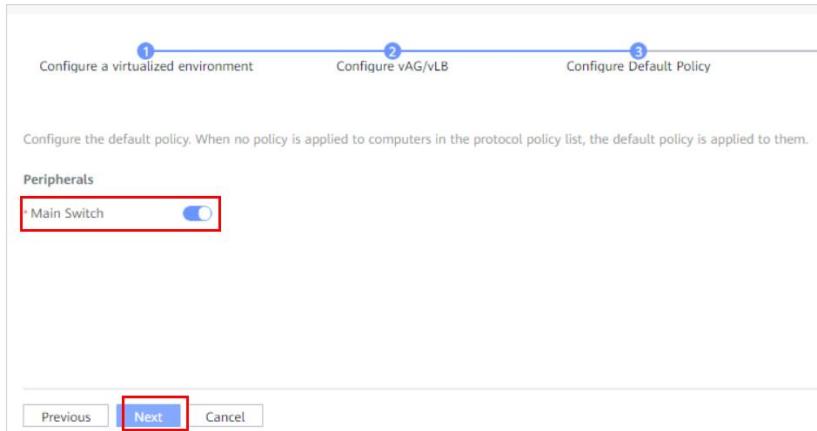
- This operation is required only when the vAG and vLB are deployed.
- **Server IP Address:** indicates the service plane IP address of the vAG server. Enter **192.168.203.31**.
- **Deployment Type:** indicates the type of the component deployed on the VM. Select **vAG+vLB**.
- **SSH Account:** indicates the maintenance account of the vAG server, which defaults to **gandalf**.
- **Password:** indicates the maintenance password of the vAG server, which defaults to **Cloud12#\$**.

## Configuring the vAG/vLB (2)



- This operation is required only when the vAG and vLB are deployed.
- **Server IP Address:** indicates the service plane IP address of the vAG server. Enter **192.168.203.31**.
- **Deployment Type:** indicates the type of the component deployed on the VM. Select **vAG+vLB**.
- **SSH Account:** indicates the maintenance account of the vAG server, which defaults to **gandalf**.
- **Password:** indicates the maintenance password of the vAG server, which defaults to **Cloud12#\$**.

## Configuring a Default Policy



- Configure the default policy for peripherals.
  - By default, **Main Switch** for peripherals is enabled, and all peripherals can be directly used. You can modify the default policy.

## Confirming the Information

The screenshot shows a software interface for configuring a virtualized environment. The top navigation bar has five steps: 1. Configure a virtualized environment, 2. Configure vAG/vLB, 3. Configure Default Policy, 4. Confirm, and 5. Configuration Complete. The current step is 'Confirm'.  
  
The main area is divided into sections:

- Virtualization environment configuration:**

Type: FusionCompute	FusionCompute IP Address: 192.168.104.30	FusionCompute Port Number: 7070
SSL Port Number: 7443	User: vdisysman	Protocol: https
Description:		
- vAG/vLB Information:**

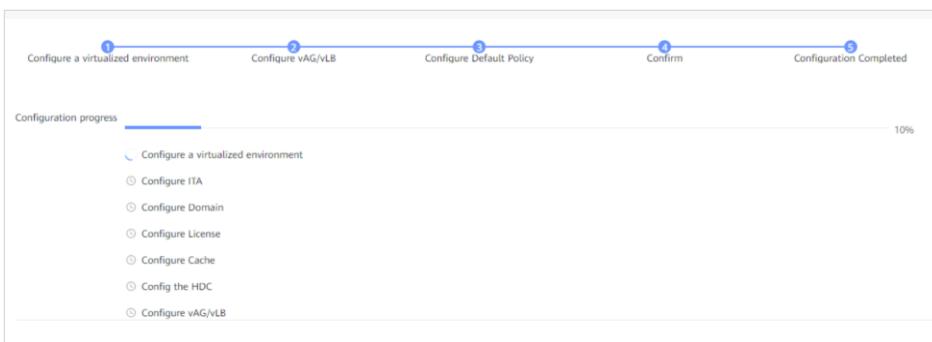
IP Address: 192.168.105.11	Deployment Type: vAG+vLB	Description:
----------------------------	--------------------------	--------------
- Default Policy Configuration:**

Peripherals:
--------------

At the bottom are three buttons: Previous, Next (highlighted in blue), and Cancel.

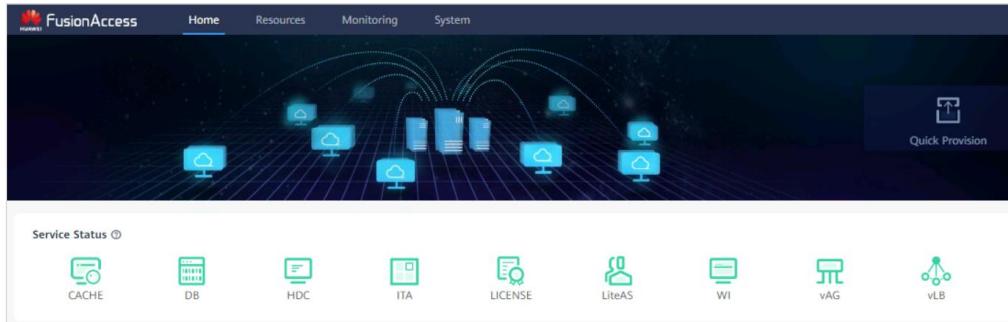
- After the initial configuration is complete, you are advised to change the passwords of all accounts once every three months to ensure system security.

# Completing the Configuration (1)

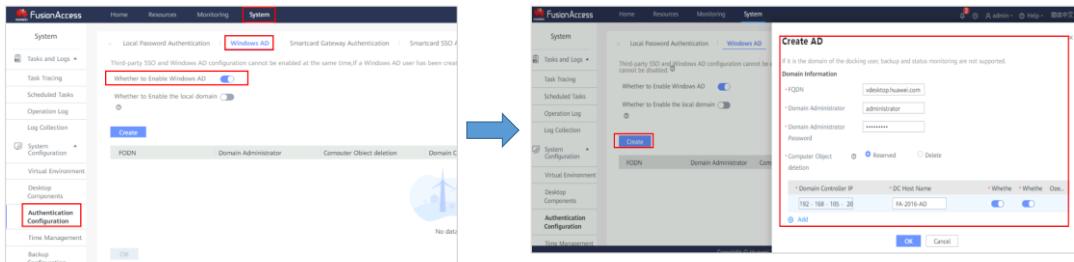


- After the configuration is complete, the FusionAccess system page is displayed.

## Completing the Configuration (2)



# Configuring the Connection to Windows AD (1)



73      Huawei Confidential



- **Whether to Enable Windows AD:** Enable this function.
- **FQDN:** name of the Windows AD domain controller
- **Domain Administrator:** name of the administrator who accesses the Windows AD server
- **Domain Administrator Password:** administrator password for login
- **Domain Controller IP:** service plane IP address of the Windows AD server
- **DC Host Name:** host name of the Windows AD server, for example, FA-2016AD-01

## Configuring the Connection to Windows AD (2)

Local Password Authentication | **Windows AD** | Smartcard Gateway Authentication | Smartcard SSO Authentication | Two-Factor Authentication | Third-Party Password | Local T

Third-party SSO and Windows AD configuration cannot be enabled at the same time, If a Windows AD user has been created, the Whether to Enable Windows AD switch cannot be disabled. ⓘ

Whether to Enable Windows AD

Whether to Enable the local domain

**Create**

FQDN	Domain Administrator	Computer Object deletion	Domain Controller IP	DC Host Name	DNS
vdesktop.huawei.com	vdadmin	Reserved	192.168.105.20	FA-2016-AD	192.168.105.20

# 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。

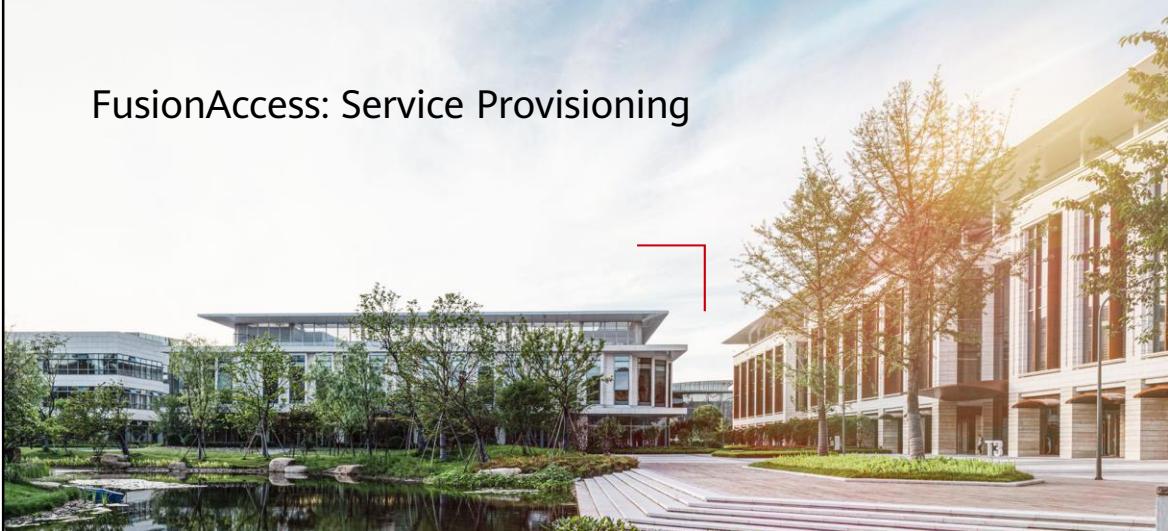
Bring digital to every person, home, and  
organization for a fully connected,  
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



## FusionAccess: Service Provisioning



# Foreword

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

# Objectives

- Upon completion of this course, you will understand:
  - Principles of full copy and linked clone
  - Differences between full copy, linked clone, and QuickPrep
  - Process for creating a VM template
  - Process for provisioning a virtual desktop

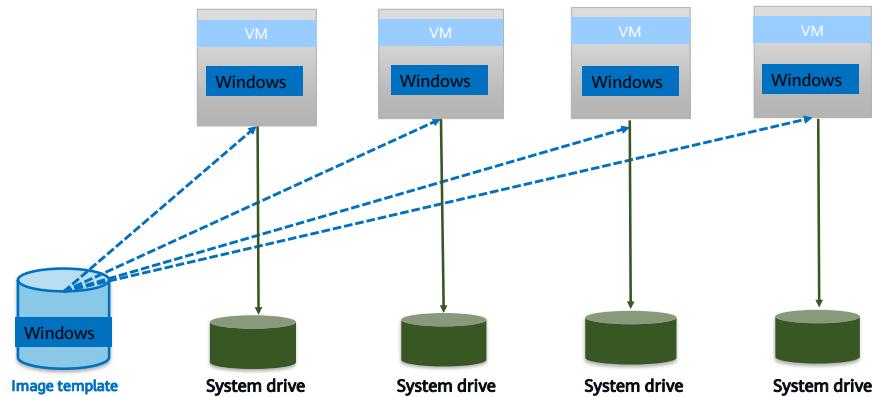
# Contents

- 1. Service Encapsulation**
2. Template Creation
3. Virtual Desktop Provisioning

## Background of Clone

- Virtual desktop technologies enable the batch provisioning and O&M of office desktops, and make enterprise IT management easier. Clone is one important technology. Administrators clone a parent VM/template on 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, and QuickPrep derived from full copy.

## A Full Copy Desktop



- For 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.

## Principles of Full Copy

- A full copy VM is a complete and independent copy of a parent VM (VM template). It is independent of the parent VM - modification and deletion of the parent VM do not affect the running of the full copy VM.

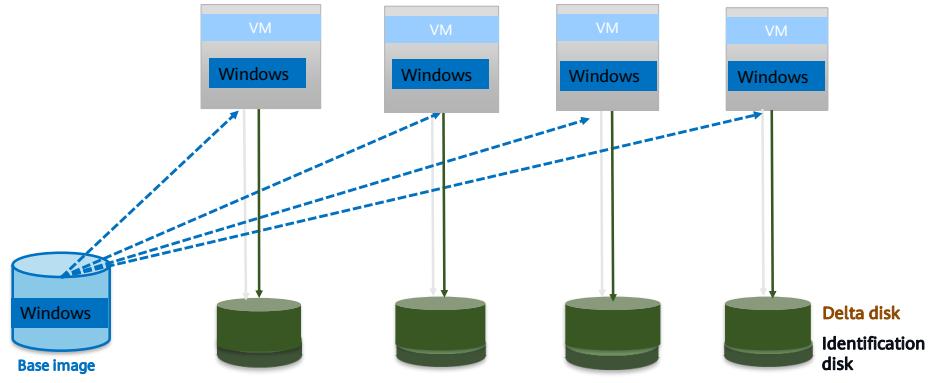
## Characteristics of Full Copy

- Each full copy VM is an independent entity, and data changes (such as software installation) on each VM can be saved.
- However, both the parent VM and each full copy VM use independent CPU, memory, and disk resources. Users need to maintain software (such as upgrades or antivirus updates) on each full copy VM.

## 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

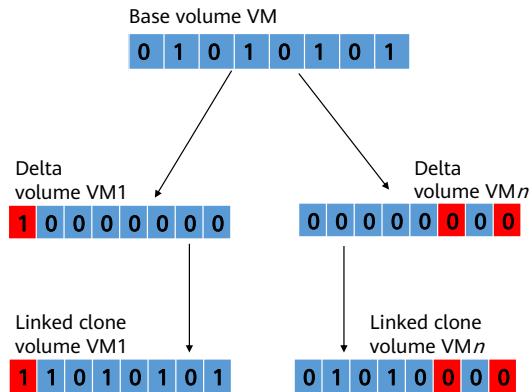


Higher management efficiency   Faster creation   Lower storage costs  
Currently, linked clone is a mainstream desktop virtualization mode.

- Technical highlights:
  - Multiple linked clones running the same OS share one base image, which can be ungraded and maintained in a unified manner.
  - Delta data is stored on linked clones.
  - Automatic restoration upon shutdown is supported.
  - Storage costs are reduced by 60%.
  - It takes only 12 seconds to create a linked clone VM. (Test data)
- Application scenarios:
  - Task-based desktops or scenarios where only customized data is available but no customized program is available (Temporary customized programs are available before the base image is updated.)

## Principles of Linked Clone

- The data in both the base and delta volumes consists of the data in the linked clone volume. 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. 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

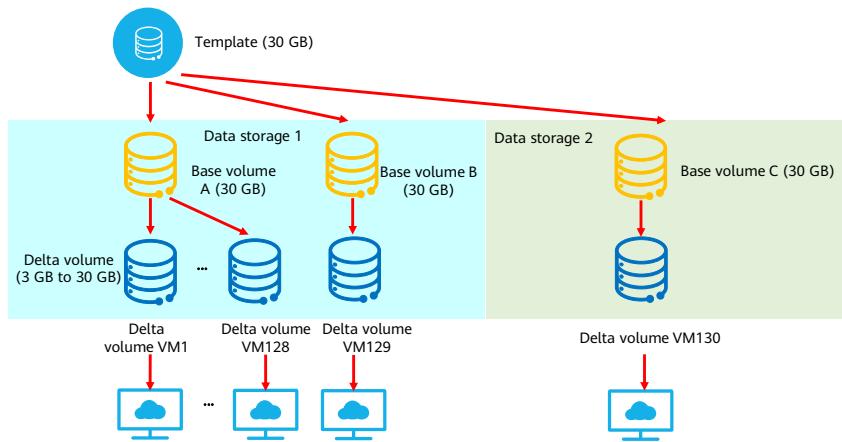
- Administrators upgrade multiple systems and install system patches and new software for linked clone VMs together.
- A shared base disk means no need to copy the system disk.
- The delta disks of the linked clone VMs store temporary user data, which can be automatically deleted when the VMs are stopped.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

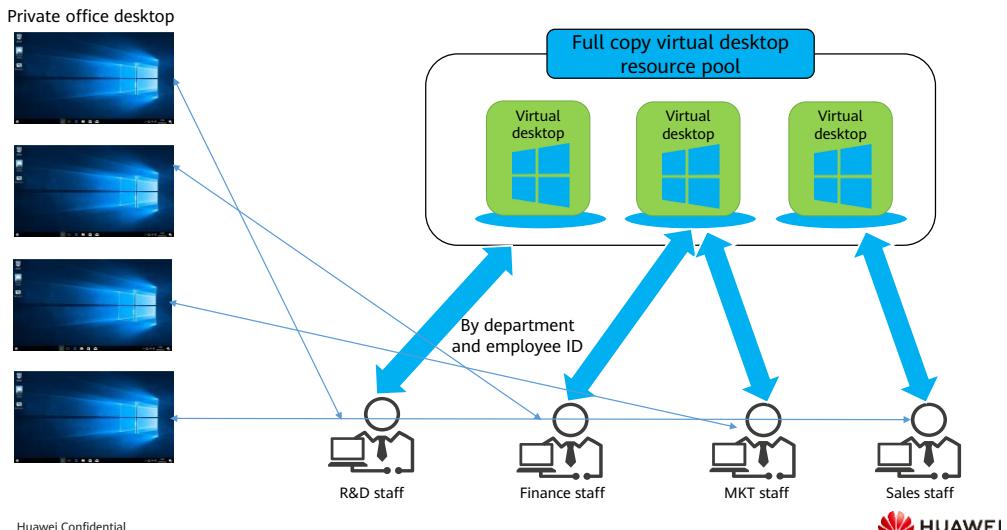
- Linked clone improves efficiency and saves costs.
  - VMs can be created in seconds, so overall provisioning is faster.
  - A large amount of storage space can be saved, lowering enterprise IT costs.
  - Unified system updates and patch installation for linked clone VMs make O&M more efficient and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

## Full Copy Use Case: Personalized Office

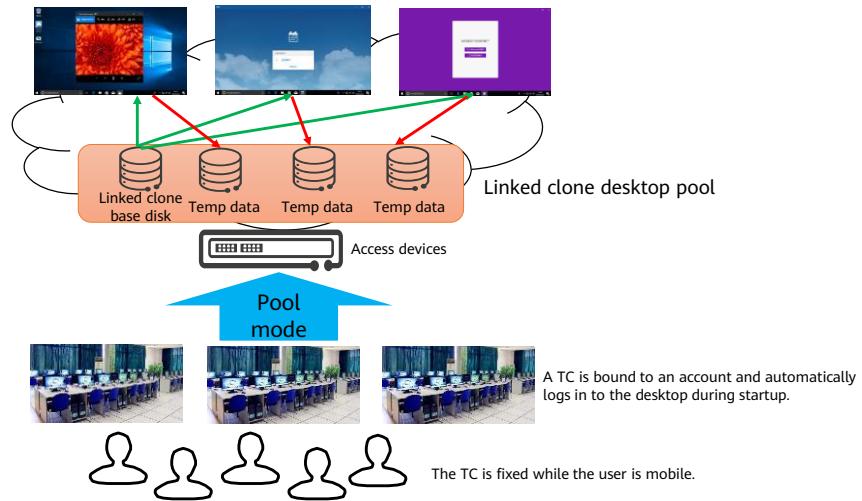


15    Huawei Confidential



- 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



16      Huawei Confidential

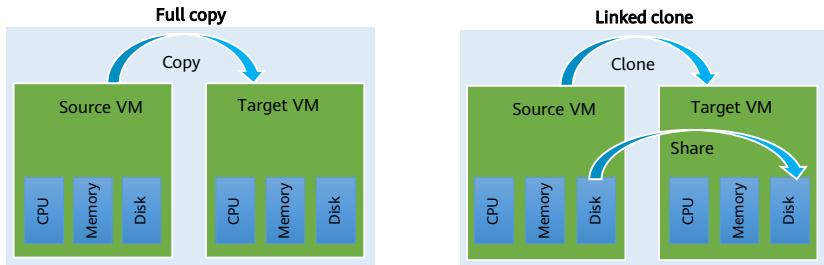


- In an electronic reading room, users only need to log in to and use VMs. The reading software has been contained in image files, and the service is simple. An electronic reading room has the following characteristics:
  - Users can access the Internet, but the viruses and Trojan on the network are 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.

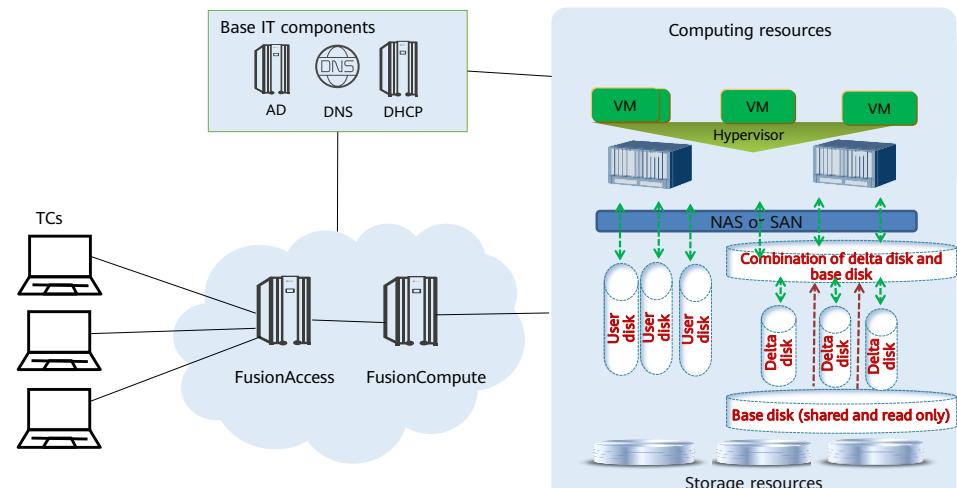


17      Huawei Confidential

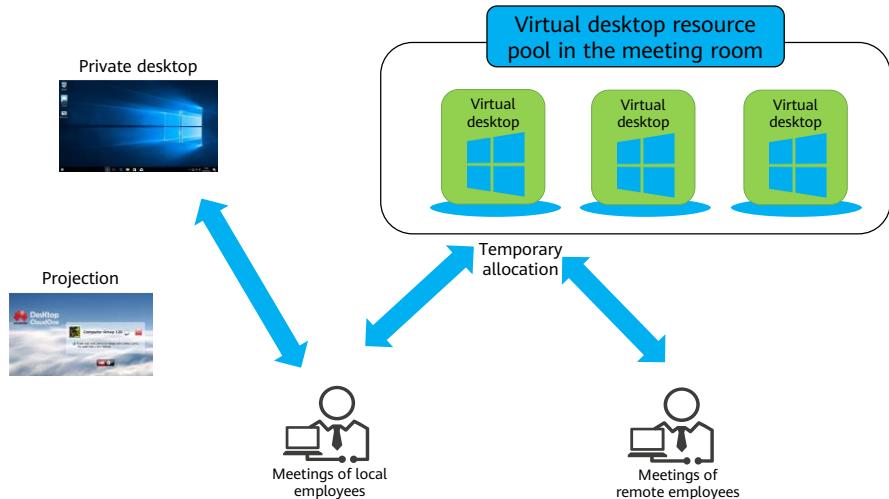
 HUAWEI

- 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.

## Full Copy vs Linked Clone (2)



## Full Copy and Linked Clone Hybrid Use Case: Routine Office



19      Huawei Confidential



- 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.

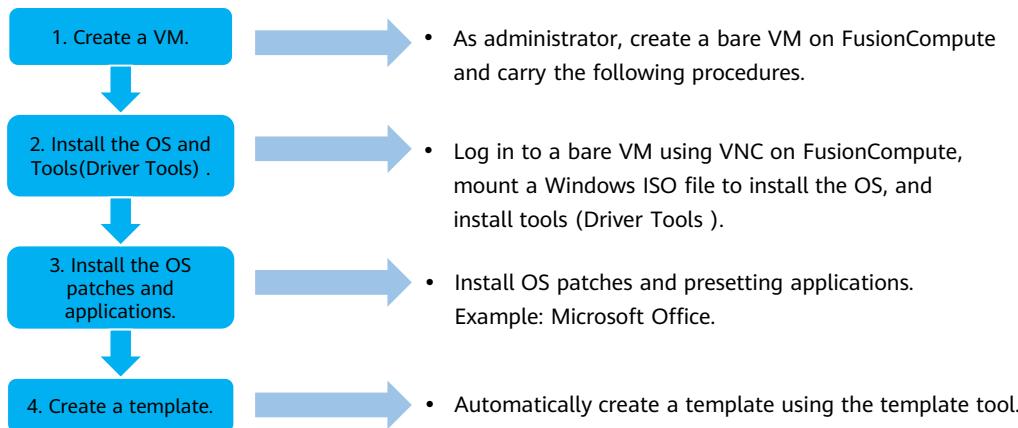
## Comparison of Desktop VMs

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

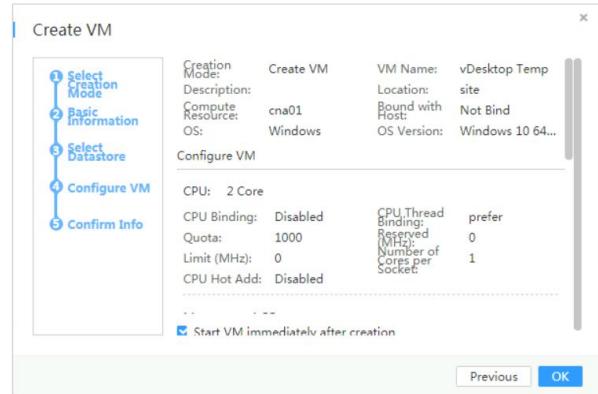
1. Service Encapsulation
- 2. Template Creation**
3. Virtual Desktop Provisioning

## Creating a Template



## Creating a Bare VM

- Log in to FusionCompute, click **Resource Pools**, choose the target cluster to create a bare VM.



## Installing the OS (1)

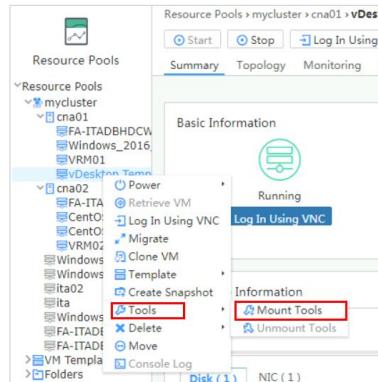
- Log in to the template VM using VNC, mount the ISO file, and install the OS.

The screenshot shows a 'Basic Information' panel for a virtual machine named 'vDesktop Temp'. The machine is currently 'Running' and has a status bar indicating 'Log In Using VNC'. The detailed configuration includes:

Category	Value
Name	vDesktop Temp
Created At	(empty)
Type	Common VM
IP Address	0.0.0.0
Initial System Password	View
Bind with Host	No
Description	(empty)
ID	i-00000051
OS Type	Windows 10 64bit
Working Location	autoDS_cna01
Cluster	mycluster
CPU Architecture	X86
UUID	df03ef09-fb8d-4d7e-89fd-560f52621ee4
Tools	Not Running
IMC Mode	Disabled
Host	cna01

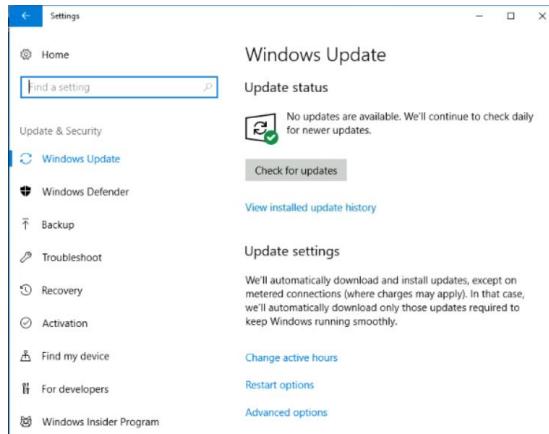
## Installing the OS (2)

- On FusionCompute, choose **Mount Tools** to mount the Driver Tools to the VM and install the Driver Tools using VNC.



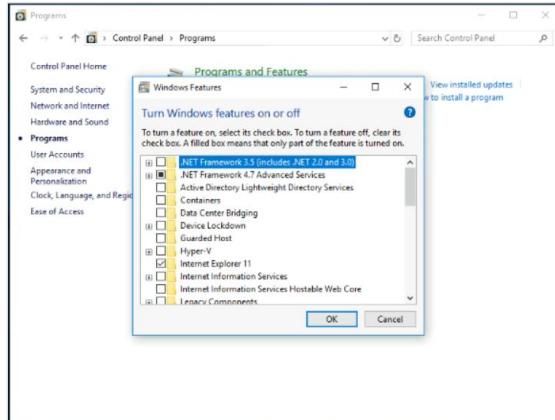
# Installing OS Patches and Applications (1)

- Install OS patches.



## Installing OS Patches and Applications (2)

- Pre-install the required applications in the template.

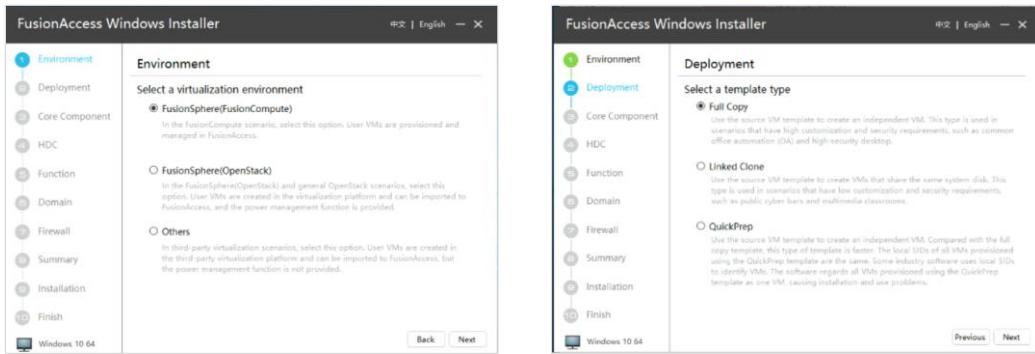


## Creating a Template Using the Tool

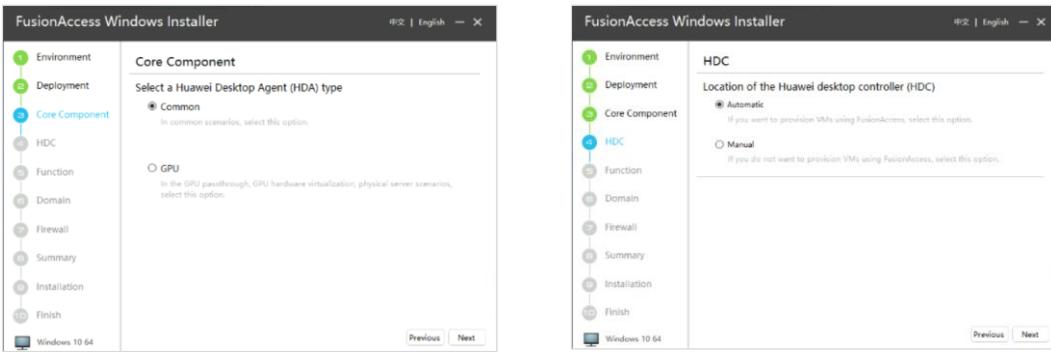
- Log in to the VM.
- Mount **FusionAccess\_WindowsDesktop\_Installer\_8.0.2.iso** to the VM.
- Open the virtual drive and double-click **run.bat** to start the template creation tool.
- Click **Create Template** and create a template as prompted.
- Unmount the virtual drive and shut down the VM.



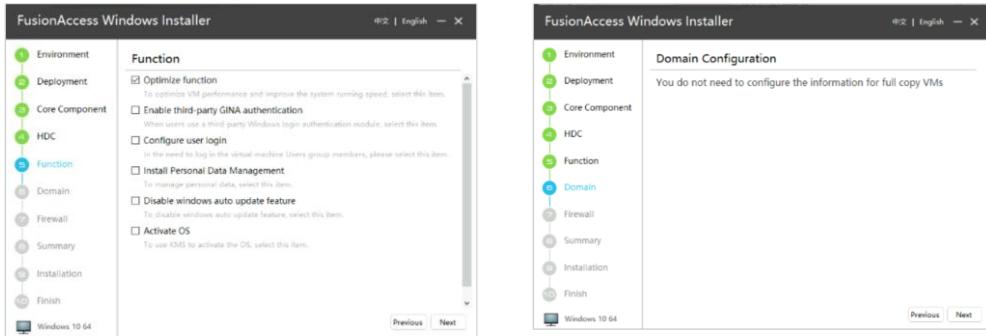
# Creating a Full Copy Template (1)



## Creating a Full Copy Template (2)



## Creating a Full Copy Template (3)



## Creating a Full Copy Template (4)

The image displays two screenshots of the FusionAccess Windows Installer interface.

**Left Screenshot (Firewall Step):**

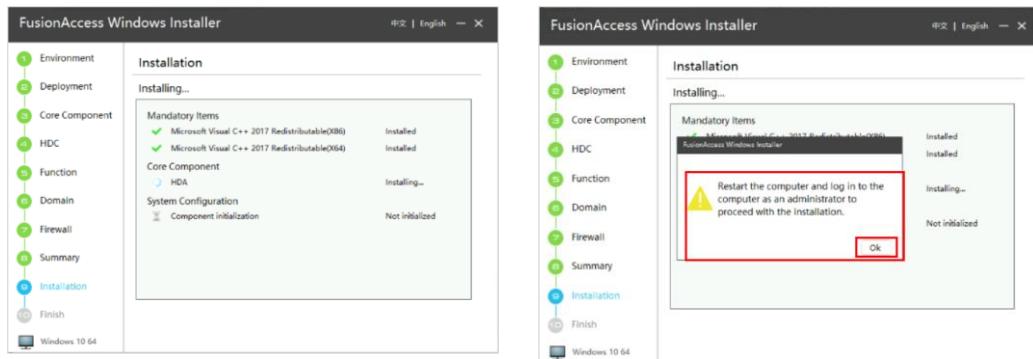
- Left Panel:** Shows the navigation path: Environment, Deployment, Core Component, HDC, Function, Domain, Firewall (highlighted), Summary, Installation, and Finish.
- Right Panel:** Title: Firewall. Subtitle: The default ports are as follows. A table lists default ports:

135	TCP	6001	UDP
3389	TCP	6040	UDP
6781	TCP	6041	UDP
6791	TCP	49152-65535	UDP
28111	TCP&UDP		
28512	TCP		
28521	TCP		
28522	TCP		
49152-65535	TCP		
6050	UDP		
- Bottom:** Configure firewall rules section with options: Automatic (selected) and Manual. A note: If you select this option, Windows Firewall rules can be automatically created. If Windows Firewall is not used or needs to be manually configured, select this option.
- Buttons:** Previous and Next.

**Right Screenshot (Summary Step):**

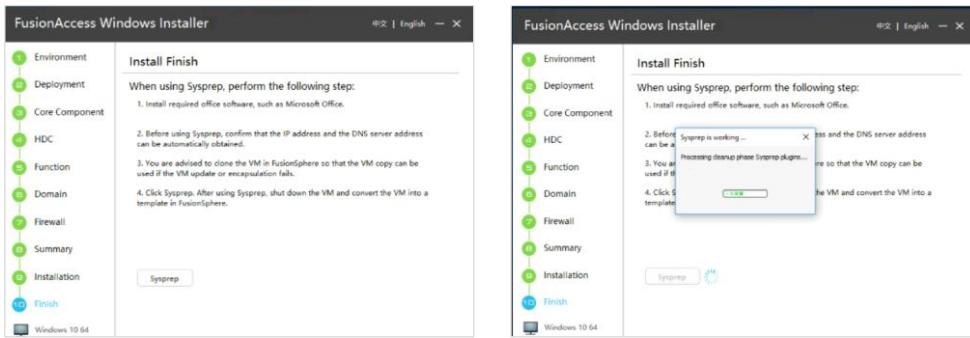
- Left Panel:** Shows the navigation path: Environment, Deployment, Core Component, HDC, Function, Domain, Firewall (highlighted), Summary (highlighted), Installation, and Finish.
- Right Panel:** Title: Summary. Subtitle: Confirm installation configuration information. It lists the following configuration:
  - Virtualization Environment: FusionSphere/FusionCompute
  - Deployment: Full Copy
  - Core Component: Common
  - HDC: Automatic
  - Function: Optimize function
  - Domain: You do not need to configure the information for full copy VMs
  - Firewall: Automatic
- Bottom:** Previous and Install buttons.

## Creating a Full Copy Template (5)



- After the HDA component is installed, restart the computer.
- The system initialization includes:
  - Releasing system space: disabling system restoration and hibernation, transferring virtual memory page files to other disks, uninstalling unnecessary Windows components, and disabling memory dump.
  - Changing system hardware driver: changing the system group policy, IDE driver, and computer driver.
  - Adding power supply patches to enable the system to automatically detect the power supply during startup.

# Creating a Full Copy Template (6)



Do not run the program after the encapsulation. This may cause the system to break down and the encapsulation environment to be damaged.

# System Encapsulation

- 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.

- 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

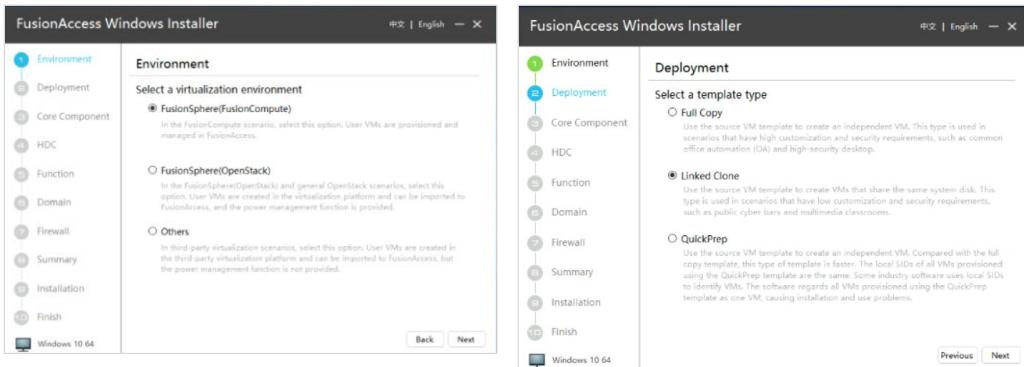
- Sysprep lets you:
  - Delete specific system data from Windows.
  - Configure entering of the audit mode for Windows on startup.
  - Configure entering of the **Welcome to Windows** page for Windows on startup.
  - Reset Windows product activation.

- 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.

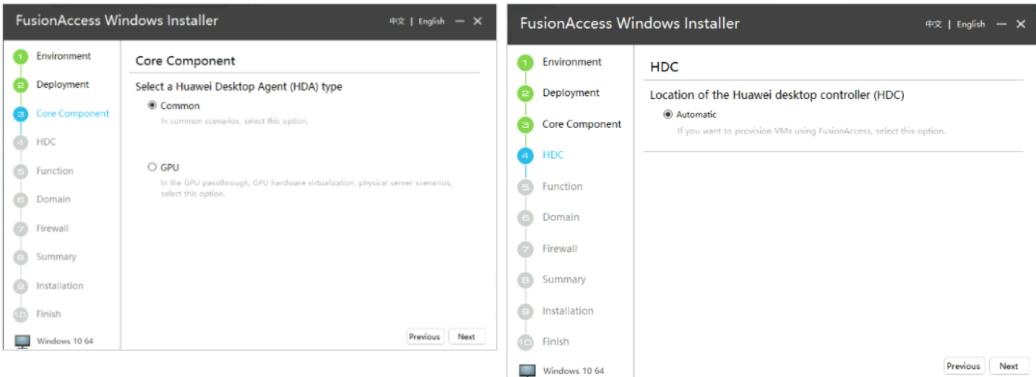
## Why Is Sysprep Necessary?

- 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.

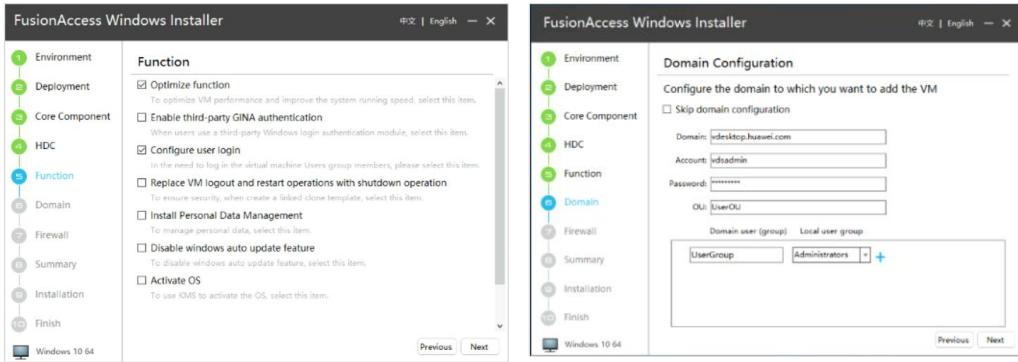
# Creating a Linked Clone Template (1)



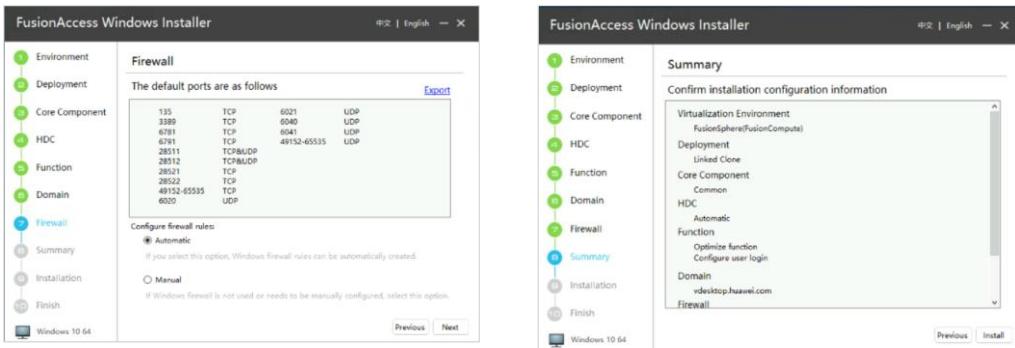
## Creating a Linked Clone Template (2)



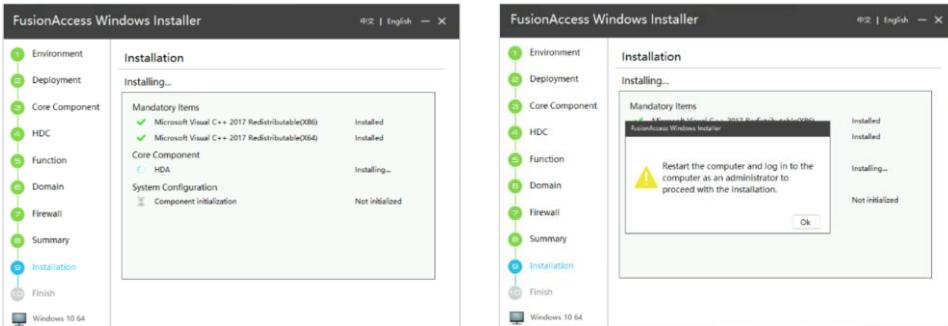
# Creating a Linked Clone Template (3)



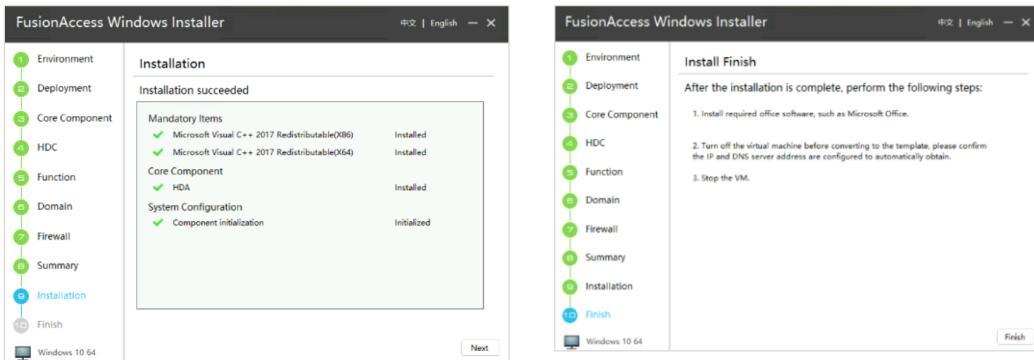
# Creating a Linked Clone Template (4)



## Creating a Linked Clone Template (5)

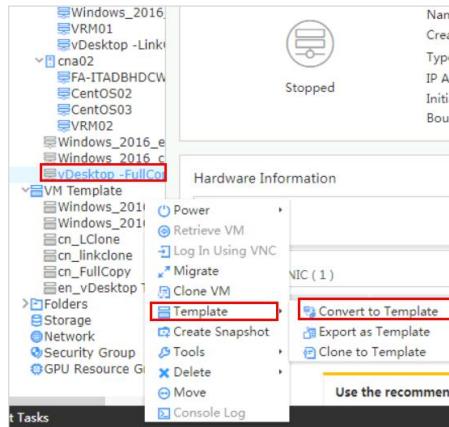


# Creating a Linked Clone Template (6)



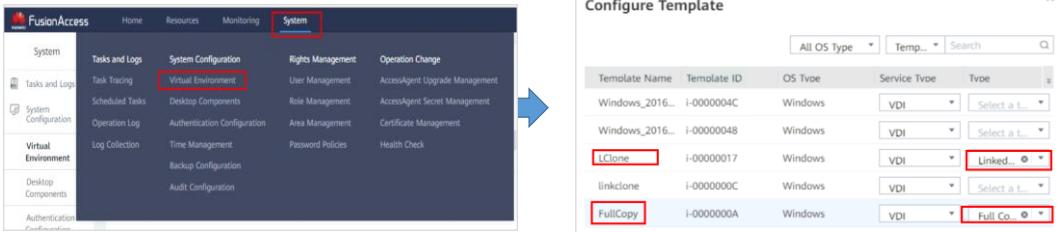
## Converting a VM to a Template

- On FusionCompute, choose **Resource Pools**, and right-click **Template > Convert to Template** in the row of the target VM.



## Configuring a Template

- On FusionAccess, choose **System > System Configuration > Virtual Environment**, click **FusionCompute** on the page displayed, and click **Operation > Template**. In the window displayed, locate the row containing the converted VM template, and configure parameters as required.

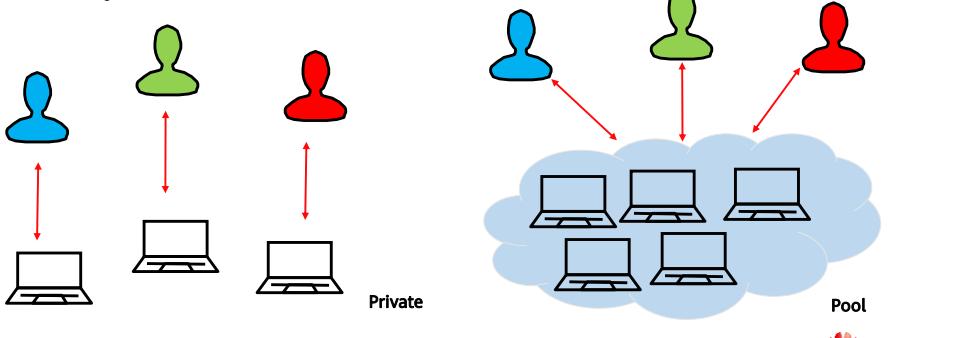


# Contents

1. Service Encapsulation
2. Template Creation
- 3. Virtual Desktop Provisioning**

## Desktop Provisioning Overview (1)

- FusionAccess has two allocation modes: private and pool.
  - Private allocation: one person has one virtual desktop. This mode is usually used in OA scenarios.
  - Pool allocation: a group of users share a group of VMs and no personalized data is stored. This mode is usually used in call center scenarios.



## Desktop Provisioning Overview (2)

- VM group types
  - Linked clone: VMs in a linked clone VM group share a system disk. This mode lets you quickly create VMs (using templates) and update applications.
  - Full copy: Each VM in a full copy VM group has a system disk. This mode lets you create VMs (using templates).

The screenshot shows a user interface for managing computer resources. On the left, there's a sidebar with 'Resources' and a dropdown menu set to 'Desktops'. Below it are buttons for 'Create' and 'Computer Groups'. The 'Computer Groups' button is highlighted with a red box. To its right is a main content area with a brief description: 'Computer groups manage computer resources by group. You can create, modify, or delete a computer group, or batch add tasks through computer groups.' Below this is a table with the following data:

Computer Group	Computer Source	Computer Type	Number of Comout...	Assigned	Assignable	Unass
FullCopy	FusionCompute	Full Copy	0	0	0	0

- Note: Before creating a VM, familiarize yourself with the terms involved in VM creation.
- During VM creation, different types of VMs need to be created for different types of users based on scenarios.
- VM groups are associated with desktop groups. A linked clone VM group maps to a dynamic or static pool desktop group. A full copy VM group maps to a private desktop group.
- VMs need to be added to the specified VM group when creating them.
- VMs need to be added to the specified desktop group when assigning them.

## Desktop Provisioning Overview (3)

- Desktop group types
  - Dynamic pool: Linked-clone VM groups dynamically assign VMs to users (one VM per user).
  - Static pool: Linked-clone VM groups dynamically assign random VMs to users (one VM per user) who attempt to log in to the desktop group for the first time.
  - Private: If the VM group type is full copy, the desktop group type is private. Users are either Static Multiple or Single.

A desktop group is a group of computers that are allocated to users or user groups.							
Create		Batch Assign					
Desktop Group ...	HDC	Desktop Group T... FullCopy_Desktop	HDC	Computer Type Private	Number of Compu... 0	Ready 0	Using 0
All desktops	All sources	All computers	All desktops	All sources	All computers	All desktops	All sources

- Linked clone pool-based desktops can be in a dynamic or static pool.
  - Dynamic pool: A user group corresponds to a desktop pool, but VMs of the pool are randomly assigned to users. Each user has access to any ready VM in the desktop pool.
  - Static pool: A user group corresponds to a desktop pool. VMs of the pool are randomly assigned to users at first. However, after a user logs in to a ready VM for the first time, the VM will be bound to the user.
- For linked clone pool-based desktops, the VM can be automatically restored upon shutdown. Administrators can configure whether to enable the automatic restoration upon shutdown. If the automatic restoration upon VM restart or logout is required, the VM OS policy needs to be modified to convert restart and logout to shutdown when the linked clone template is created.
- The corresponding pool-based desktop group supports VM prestart. Administrators can configure the prestart function on VMs in different peak or off-peak hours to ensure that some idle VMs are in the ready state. These VMs can respond to new users' login requests in a timely manner, improving user experience at lower energy costs. In addition, the pool-based desktop group supports the configuration of standby VM groups. When desktops in the pool are insufficient, VMs in standby VM groups are added to the pool in a timely manner.

## Desktop Provisioning - Quick Provision

- 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.



## Quick Provision - Creating a Computer

- Step 1: Create a computer.
  - VM group name
  - Template
  - Memory
  - Network
  - Domain name
  - VM naming rules
  - Number of computers to create

Quick Provision

1 Create Computer      2 Asian Computer      3 Confirm      4 Finish

To assign existing computers, choose Resources > Desktops > Desktop Groups

**Computer Group**

\* Computer Group  Existing Computer Group  New Computer Group

\* Computer Group Name

\* Computer Type  Full Copy  Linked Clone

**Configure**

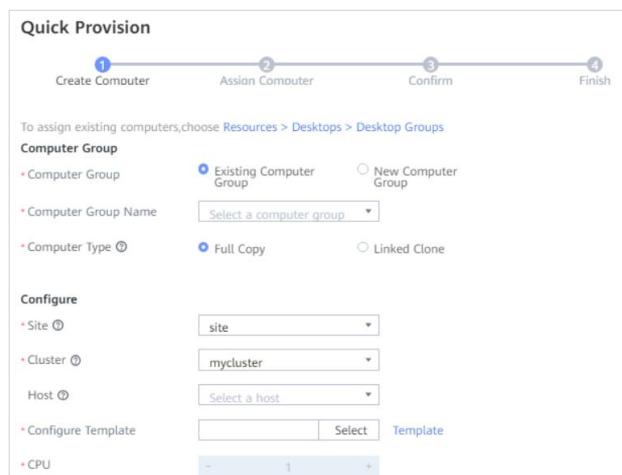
\* Site

\* Cluster

Host

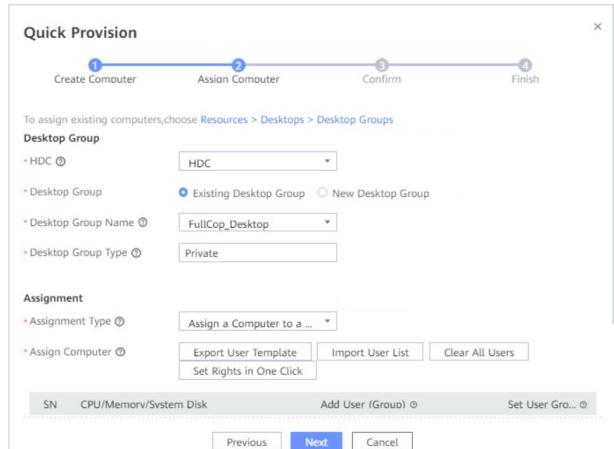
\* Configure Template

\* CPU



## Quick Provision - Assigning a Computer

- Step 2: Assign a computer.
  - Desktop group name and type
  - Assignment type and VM assignment



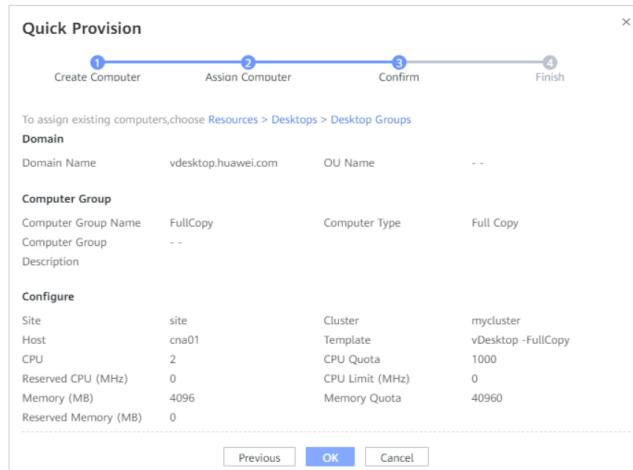
52      Huawei Confidential



- Desktop Group > Desktop Group Type (Private) > Assignment Type (Assign a Computer to a User/Assign a Computer to Multiple users)
- Desktop Group > Desktop Group Type (Static Pool/Dynamic Pool)
- The administrator specifies a user for the created VM.

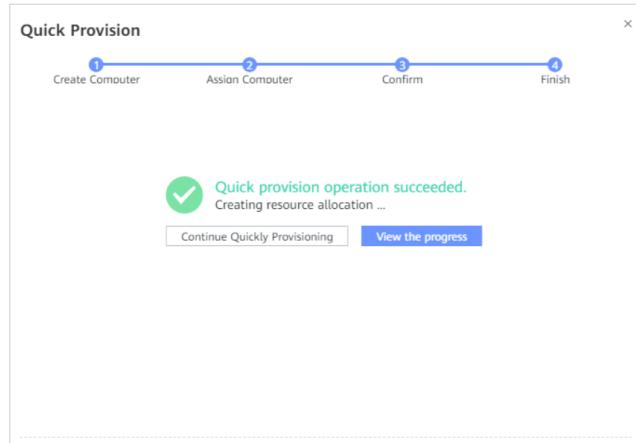
## Quick Provision - Confirming the Information

- Step 3: Confirm the information.



## Quick Provision - Finishing the Process

- Step 4: Finish the process.



## Quick Provision - Viewing a Task

- Administrators can monitor task progress in the task center.

The system business runs in the form of a task. This page manages all tasks of the system, and the page is refreshed once in 30s.

Task Type	Start Time	Progress	Status	End Time	Created By	Number ...	Number ...	Number ...	Subta...	View	Operation
Quick Pr...	2023-09-01 10:00:00	5%	Executing		admin	2	0	0	2	<a href="#">View</a>	<a href="#">Operation</a>

Object	Target ...	User	Site	IP Addr...	MAC Adr...	Start Ti...	Progress	Result	Task St...	End Time	Help
i-0000...	VDESKT...		site				<div style="width: 22%;">■</div>	In proce...	Creatin...		<a href="#">Operation</a>
i-0000...	VDESKT...		site				<div style="width: 22%;">■</div>	In proce...	Creatin...		<a href="#">Operation</a>

## 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.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



## FusionAccess: Features and Management



# 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 FusionAccess policy management, service adjustment and alarm handling.

# Objectives

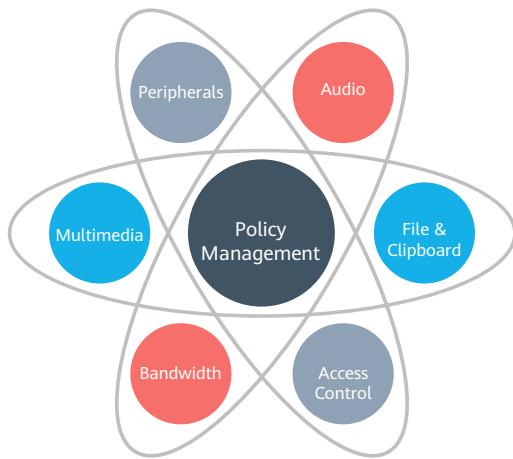
- Upon completion of this course, you will understand:
  - Policy management
  - Methods of service adjustment
  - Methods of alarm handling

# Contents

- 1. Policy Management**
2. Service Adjustment
3. Alarm Handling

## 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.

## 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.

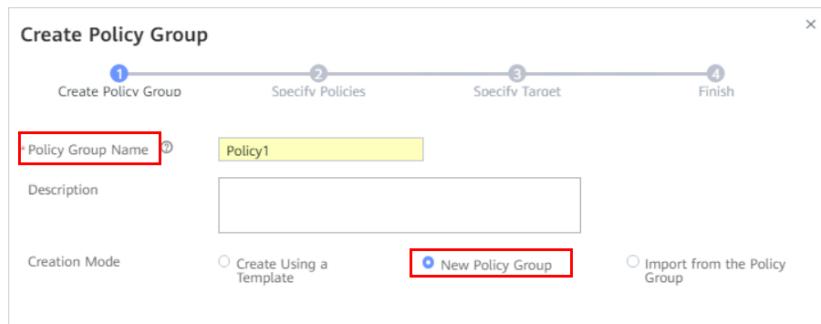
## Hands-on Practice - File Redirection (1)

- On FusionAccess, choose **Resources > Policies > Protocol Policies**, and click **Create**.

The screenshot shows the FusionAccess interface with the 'Protocol Policies' creation screen. The top navigation bar includes 'Home', 'Resources' (which is selected and highlighted in red), 'Monitoring', and 'System'. Below the navigation is a descriptive text: 'The protocol policy provides customized configuration to meet users basic OA requirements.' A 'Create' button is prominently displayed in a blue box with a red border. To the right of the 'Create' button are two smaller buttons: 'Publish All Policies to HDC' and 'Configure Default Policy'. The main area is titled 'Protocol Policies' and contains a table with columns: 'Policy Group Name', 'Update Time', and 'Desc'. On the left side, there is a sidebar under the 'Resources' heading with categories: 'Desktops', 'Computers', 'Computer Groups', 'Desktop Groups', 'Users', 'Policies' (which is selected and highlighted in red), and 'Protocol Policies' (which is also highlighted in red). Below these are 'Access Control Policies' and 'Terminal and User Binding Policies'.

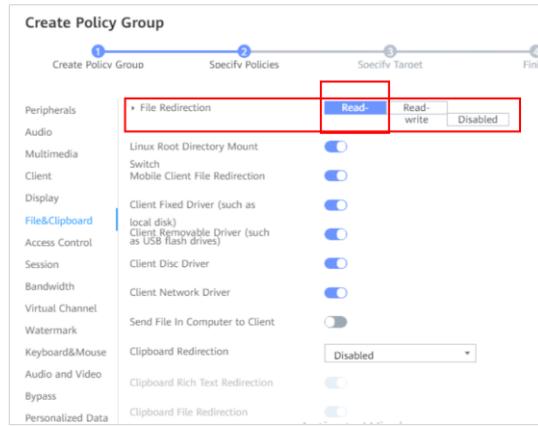
## Hands-on Practice - File Redirection (2)

- Step 1: Create a policy group.



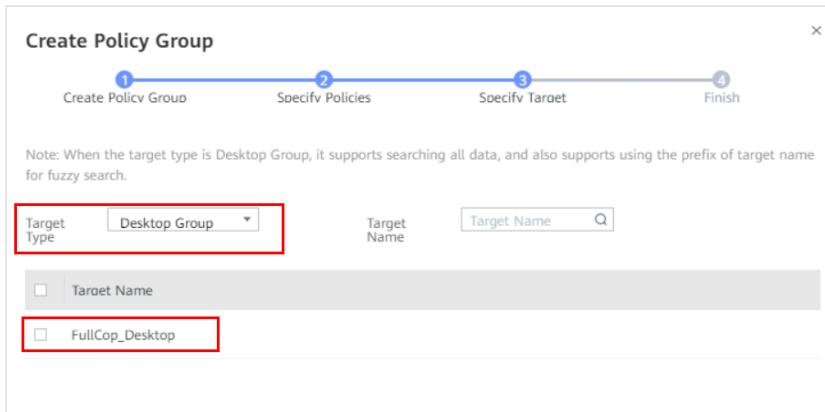
## Hands-on Practice - File Redirection (3)

- Step 2: Specify a policy.



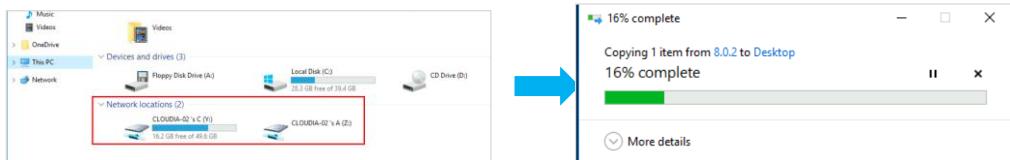
## Hands-on Practice - File Redirection (4)

- Step 3: Specify a target.



## Hands-on Practice - File Redirection (5)

- Verification
  - Log in to the virtual desktop as user **vdsuser**. Click **This PC** and ensure that the disk drive on the local client is redirected to the virtual desktop.
  - Copy a file from the local drive on the client and paste it to the drive of the virtual desktop. Check that the operation is successful.



# Contents

1. Policy Management
- 2. Service Adjustment**
3. Alarm Handling

## Service Adjustment - Modifying Computer Specifications (1)

- On FusionAccess Web Client, choose **Resources > Desktops > Computers**, find the computer to modify, and choose **Operation > Power > Stop**. Wait for the running status to change to **Stopped**.

Name	ID	IP Address	Running Status	Assignment Type	User (Group)	Login Status
vdesktop\FULLC...	i-00000054	192.168.105.106	Running	Assign a compu...	VDESKTOP\vd...	Ready
vdesktop\FULLC...	i-00000055	192.168.105.105	Running	Assign a compu...	VDESKTOP\vd...	Using

13    Huawei Confidential



- In office scenarios, users can change virtual desktop specifications to meet actual needs.
- Note:
  - 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.

## Service Adjustment - Modifying Computer Specifications (2)

- On the **Computers** page, select the computer to modify and choose **Operation > Change > Modify Computer**. After the modification is complete, restart the computer.

The screenshot shows the 'Computers' page in FusionCompute. There are two entries in the list:

Name	ID	IP Address	Running Status	Assignment Type	User (Group)	Login Status
vdesktop(FULLC...)	i-00000054	192.168.105.106	Stopped	Assign a compu...	VDESKTOP\vd...	Ready
vdesktop(FULLC...)	i-00000055	192.168.105.105	Running	Assign a compu...	VDESKTOP\vd...	Using

A context menu is open over the second entry (ID i-00000055). The 'Modify Computer' option is highlighted with a red box. Other options in the menu include Recompose Svst..., Restore System..., Set, Choose Area, Delete, and Update AccessA..., Update Authenti..., and Update SID.

## Service Adjustment - Adding a Computer Domain User (1)

- To add a user, **Assignment Type** must be set to **Assign a Computer to Multiple Users**.

The screenshot shows a table of assigned computers. One row is selected, and a context menu is open next to it. The menu includes options like Detach, Power, Assignment Rela..., Session, Change Desktop..., Add User, Delete User, Restore Attachm..., and Delete. The 'Assignment Rela...' option is highlighted with a red box.

Name	ID	IP Address	Running Status	Assignment Type	User (Group)	Login Status
vdesktop\HW-B...	i-00000058	192.168.105.109	Running	Assign a compu...	VDESKTOP\vd...	Ready
vdesktop\FULLC...	i-00000057	192.168.105.108	Running	Assign a compu...		
vdesktop\FULLC...	i-00000056	192.168.105.107	Running	Assign a compu...		
vdesktop\FULLC...	i-00000054	192.168.105.106	Stopped	Assign a compu...		
vdesktop\FULLC...	i-00000055	192.168.105.105	Running	Assign a compu...		

- 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 for using the computer. This operation 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.

## Service Adjustment - Adding a Computer Domain User (2)

- To add a user whose information has been configured in **Resources > Users > Domain Users**, search for the username. Select it from the results list and click **OK**.
- Specify the added user's user group. If the user group **Users** was configured during the computer template creation, set this parameter to **Users**. Otherwise, set it to **Administrators**.

Add User

Computer Name: vdesktop\FULLCOPY004

Template: i-00000052

CPU/Memory/System Disk: 2Number/4096 MB/40 GB

User: VDESKTOP\vduser01

+ Add User:  **Select**

+ Set User Group:

# Service Adjustment - Adding a Computer (1)

- Adding a computer to a computer group
  - On the **Computer Groups** page, choose **Operation** in the row of the target computer and click **Add Computer** to complete the configuration as required.

The screenshot shows the FusionAccess interface. On the left, under 'Resources', the 'Computer Groups' section is selected. It displays a table with one row: 'FullCopy' (Computer Name), 'FusionCompute' (Computer Source), 'Full Copy' (Computer Type), and two columns of zeros (Number of..., Assigned, Unassignable, Processing). A context menu is open over this row, with 'Add Computer' highlighted. To the right, a 'Add Computer' dialog box is displayed, showing the 'Computer Group' tab. It has fields for 'Computer Group Name' (FullCopy), 'Computer Source' (FusionCompute), 'Computer Type' (Full Copy), and a 'Description' field. Below this, the 'Configure' section includes dropdowns for 'Site' (site), 'Cluster' (mycluster), and 'Host' (Select a host). There is also a 'Configure Template' section with a 'Select' button and a 'Template' dropdown. At the bottom of the dialog are 'Next' and 'Cancel' buttons.

- You can 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 in a desktop group.

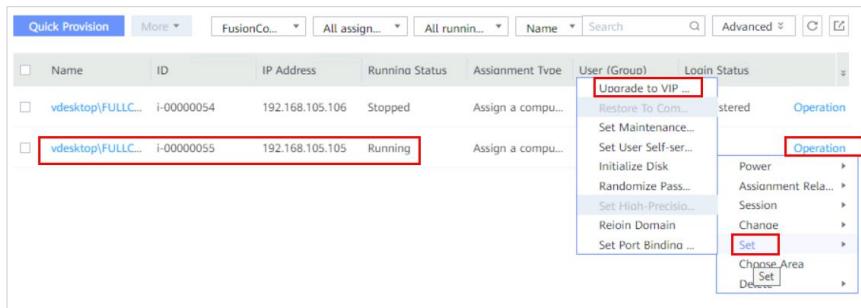
## Service Adjustment - Adding a Computer (2)

- Assigning computers to a desktop group
  - Choose **Operation** in the row of the target desktop group, and click **Assign Computer** to complete the configuration as required.

The image shows two windows side-by-side. On the left is a list of desktop groups with one item selected ('FullCopy...'). A context menu is open over this item, with the 'Assign Computer' option highlighted and surrounded by a red box. On the right is the 'Assign Computer' dialog box. It contains fields for HDC, Computer Type, Desktop Group Name, and Desktop Group Type. Under the 'Assignment Type' section, 'Assign a Computer to a ...' is selected. The 'Computer Group Name' is set to 'FullCopy' and the 'Site' is set to 'site'. At the bottom, there is a table with one row showing a computer entry: 'Name' is 'vdesktop...', 'CPU/Memory' is '2Numb...', 'OS Type' is 'Windows', 'Template' is 'i-000000...', 'User' is 'vduser02@vdesk', and 'Group' is 'Add'. There is also a 'Set Rights in One Click' button.

## Service Adjustment - Upgrading a Common Desktop to a VIP Desktop

- Only assigned full copy and linked clone computers can be upgraded to VIP desktop.
- Tip: Retain default values for VIP desktop resource assurance and real-time monitoring policies for all VIP users.



19      Huawei Confidential



- 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 enjoy faster CPU and memory resource supply, real-time computer status monitoring, and better experience. Administrators can flexibly upgrade common desktops to VIP desktops as required.

## Service Adjustment - Configuring User Access Control Policies

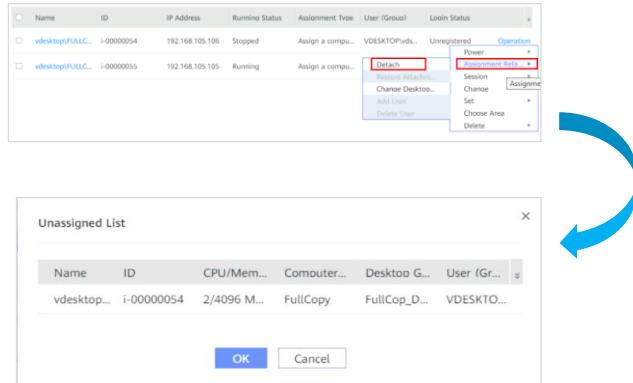
- User access control policies include:
  - Access time
  - Gateway authentication
  - Terminal and user binding
  - Terminal and desktop binding

The screenshot illustrates the configuration process for User Access Control Policies. It shows the 'Create' dialog with two main steps: 'Time Segments' and 'Select Policy Targets'. In the 'Time Segments' step, a policy named 'LP\_Time' is being configured with a single time segment from 00:00 to 08:00. In the 'Select Policy Targets' step, targets are being selected from a list, including 'FullCop/Desktop' and 'Target Name'. A sidebar on the left lists policy categories: 'Policies', 'Protocol Policies', 'Access Control Policies' (which is highlighted with a red box), 'Terminal and User Binding Policies', and 'Terminal and Desktop Binding Policies'. A blue arrow points from the 'Access Control Policies' box in the sidebar to the 'Time Segments' dialog. Another blue arrow points from the 'Time Segments' dialog to the 'Select Policy Targets' dialog. Red callout boxes provide instructions: 'Set time segments for when access is forbidden.' and 'Select policy targets.'

- In most cases, no restrictions are required to control user access. When high information security is imperative, user access control policies can be set to restrict the access time, IP address, user account, and access location.
- User access control policies include:
  - Access time control: Set multiple time segments and specify targets that are not allowed to access computers during these segments.
  - Terminal and user binding: After users and terminals are bound, users can log in to computers by using bound terminals only, ensuring the security of sensitive information in computers. The administrators can group users or terminals for batch binding.

## Service Adjustment - Unassigning Virtual Desktops

- In the FusionAccess computer list, select one or more computers to be unassigned and click OK.



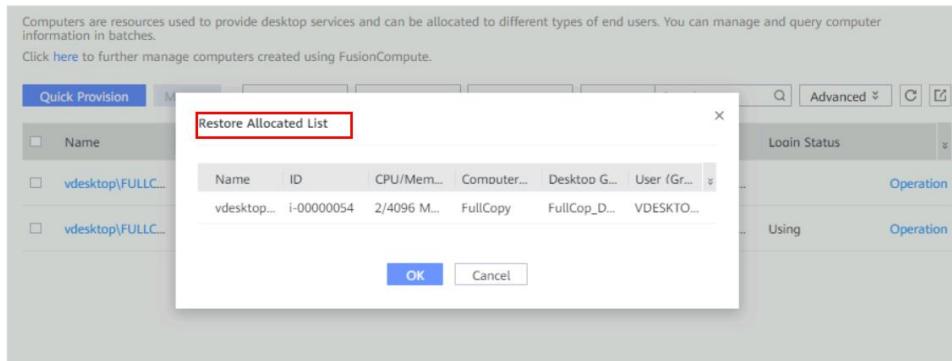
21      Huawei Confidential



- You can unassign a computer and restore assignment due to certain reasons, such as the resignation or changes in position or work scope of an employee.
- A full copy computer whose **Assignment Type** is **Assign a Computer to Multiple Users** is automatically shut down after being unassigned.

## Service Adjustment - Restoring Virtual Desktop Assignment

- Search for the unassigned computer using relevant criteria. Select the computer from the results list and choose **Operation > Assignment Relationship > Restore Attachment**.



22      Huawei Confidential



- Search for the unassigned computer using relevant criteria. Select the computer from the results list.
- Choose **Operation > Assignment Relationship > Restore Attachment**.
- In the confirmation dialog box that is displayed, click **OK**.
- In the **Restore Allocated List** dialog box, click **OK**.
- In the displayed dialog box, click **OK**.
- For a full copy computer whose **Assignment Type** is **Assign a Computer to a User**, choose **Operation > Assignment Relationship > Restore Assignment** to reassign the computer. However, the full-copy computer can only be assigned to the original user and the user group permission remains unchanged. Once the unassigned computer is assigned and started, the computer icon on the WI turns on. Wait 3 minutes before logging in.

# Contents

1. Policy Management
2. Service Adjustment
- 3. Alarm Handling**

## 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.	<p>Note: On FusionAccess Web Client, choose <b>Monitoring &gt; VIP Desktop Alarms &gt; VIP Desktop Policies</b> to configure monitoring items for VIP desktops.</p> <p>Regularly check VIP desktop alarms.</p> <p>Configure email notification to handle VIP desktop alarms in real time.</p> <p>Note: On FusionAccess Web Client, choose <b>Monitoring &gt; Alarms &gt; Email Notification</b> to configure them.</p>

- 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.

# Component Status Monitoring

- On FusionAccess Web Client, choose **Monitoring > Status Monitoring**.

The screenshot shows the FusionAccess Web Client interface with the 'Monitoring' tab selected. On the left, there's a sidebar with links: 'Monitoring' (highlighted with a red box), 'Alarms', 'VIP Desktop Alarms', and 'Reports'. The main content area displays a table of component status. A note at the top states: 'Status monitoring data is not in real time and has a deviation of about 6 minutes. The status of the installed AD, DHCP, DNS, License, HDC, WI, vAG, vLB, UNS and AUS components can be monitored. If a component is not displayed in the monitoring list, configured IP address is correct.' The table has columns for Component Name, Component IP Address, and Component Status. All components listed are in 'Normal' status.

Component Name	Component IP Address	Component Status
AD	192.168.105.20	Normal
CACHE	192.168.105.11	Normal
DB	192.168.105.11	Normal
HDC	192.168.105.11	Normal
ITA	192.168.105.11	Normal
LICENSE	192.168.105.11	Normal
LiteAS	192.168.105.11	Normal
WI	192.168.105.11	Normal
vAG	192.168.105.11	Normal
vLB	192.168.105.11	Normal

# System Alarm Monitoring

- On FusionAccess Web Client, choose **Monitoring > Alarms > System Alarms**.

The screenshot shows the FusionAccess Web Client interface with the 'Monitoring' tab selected. On the left, there's a sidebar with 'Monitoring' and 'Alarms' sections. The main area is titled 'System Alarms' and includes tabs for 'Email Notification' and 'Alarm Component Configuration'. A message at the top states: 'The Alarms module monitors and displays all alarms generated by the system and provides guidance for handling the alarms. All active alarms are displayed by default, the system automatically checks the number of alarms every seven days and clears the alarms if the number of alarms exceeds 100,000.' Below this is a search bar with dropdowns for 'Not cleared', 'All alarm s...', 'Alar...', 'Search', and 'Advanced'. A table lists two alarms:

Alarm Name	Alarm Object	Alarm Severity	Generation Time	Clear Time	Clear Type	Operation
License is not loa...	LICENSE	Critical				<a href="#">Clear Alarm</a>
Backup Server Is ...	BACKUP	Critical				<a href="#">Clear Alarm</a>

## VIP Desktop Alarm Monitoring

- Method 1: Proactively check alarms. On FusionAccess Web Client, choose **Monitoring > VIP Desktop Alarms**.
- Method 2: Configure email notification. When the VIP desktop is malfunctioning, users receive a prompt alarm email.

The screenshot shows the FusionAccess Web Client interface. The top navigation bar includes Home, Resources, Monitoring (which is selected and highlighted in red), and System. A user icon with '2' and '1' notifications is shown next to 'admin'. The left sidebar has a 'Monitoring' section with sub-options: Alarms, VIP Desktop Alarms (highlighted in red), Status Monitoring, and Reports. The main content area is titled 'VIP Desktop Policies' and contains the text: 'The VIP desktop alarm monitors the alarm information generated by the VIP desktop.' Below this is a search bar with dropdowns for 'All event types', 'Name', and a 'Search' button. A table header is visible with columns: Name, ID, User (Group), Generation Time, Send Alarm Mail, Event Type, and Resto. At the bottom of the content area is a blue circular icon with a wind turbine and the text 'No data'.

## Computer Status Statistics

- On FusionAccess Web Client, choose Home > Computer Status Statistics.



# Gateway Status Monitoring

- On FusionAccess Web Client, choose **Monitoring > Reports > vAG Information**.

The screenshot shows the FusionAccess Web Client interface with the 'Monitoring' tab selected. In the left sidebar, the 'vAG Information' option is highlighted with a red box. The main content area displays a table titled 'User Connections' with the following data:

SN	vAG Service IP	Time	Current Inbound	Current Outbound	Current CPU Usage	Current Memory Usage	Number of Connections	TCP Retrans
1	192.168.105.11	—	0.00000	0.00000	1	41	0	0
2	192.168.105.11	—	0.00000	0.00000	1	41	0	0
3	192.168.105.11	—	0.00000	0.00000	17	41	0	0
4	192.168.105.11	—	0.00000	0.00000	0	41	0	0
5	192.168.105.11	—	0.00000	0.00000	2	41	0	0
6	192.168.105.11	—	0.00000	0.00000	1	41	0	0
7	192.168.105.11	—	0.00000	0.00000	1	41	0	0
8	192.168.105.11	—	0.00000	0.00000	3	40	0	0
9	192.168.105.11	—	0.00000	0.00000	1	40	0	0
10	192.168.105.11	—	0.00000	0.00000	7	40	0	0

# 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 course has taught you how to plan and create policies for virtual desktops in FusionAccess, perform service adjustment such as adding desktop users and configuring VIP desktops, and handle alarms.

# 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.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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



# 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, and cloud native concepts.

# Objectives

- Upon completion of this course, you will understand:
  - Basic concepts and component architecture of OpenStack
  - Basic concepts of edge computing
  - Basic concepts of blockchain
  - Basic concepts of cloud native and its applications

# Contents

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

## OpenStack Concepts

- OpenStack is free software and an open-source project jointly developed by Rackspace and NASA and authorized by the Apache License. **It aims to provide software services for the construction and management of public and private clouds.**

OpenStack is a solution for cloud platform deployment.



 HUAWEI

- What Is OpenStack? OpenStack is a cloud operating system that controls large-scale computing, storage, and network resource pools through data centers. The administrator can perform all management operations on the front-end interface. In addition, end users can deploy resources on the web interface.
- OpenStack is an open-source project based on a community. It provides an operation platform and tool set for cloud deployment. It aims to help organizations run clouds that provide virtual computing or storage services and to provide scalable and flexible cloud computing for public and private clouds of all sizes.

# OpenStack Design Ideas

## Open

- Remain open-source, and reuse as many existing open-source projects as possible.
- No reinvention of the wheel

## Flexible

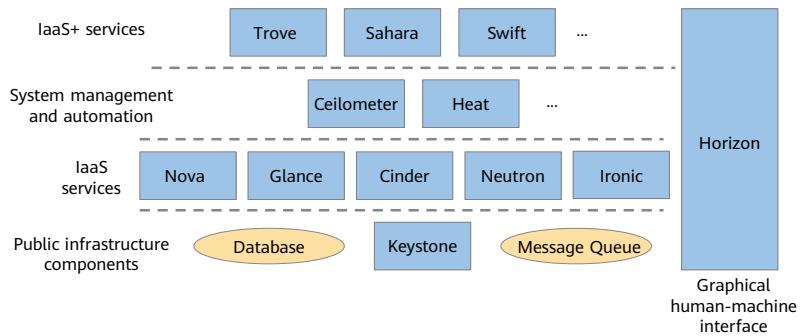
- Do not use any irreplaceable component that is private or commercial.
- Design and implement architectures using plug-ins.

## Scalable

- Multiple independent projects
- Multiple independent service components
- Decentralized architecture
- Stateless architecture

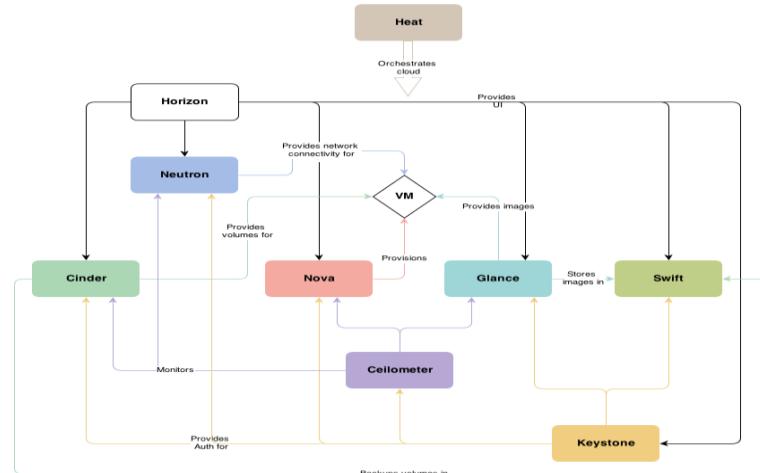
## Project Layering in OpenStack Community

- To implement cloud computing functions, OpenStack divides developments in computing, storage, and networks into separate projects. Each project corresponds to one or more OpenStack components.



- OpenStack covers general service types at the IaaS layer, some system management and automation services, and some important IaaS+ services.

## Logical Relationships in OpenStack Core Services



8 Huawei Confidential



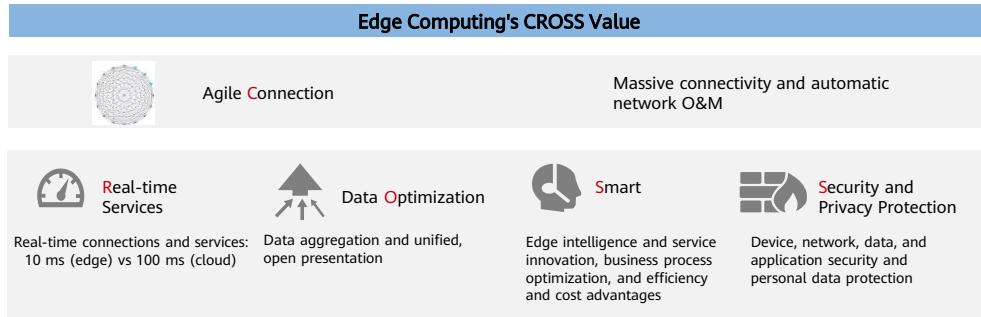
- Horizon provides a web-based self-service portal to interact with OpenStack underlying services, such as starting an instance, assigning IP addresses, and configuring access control.
- Nova manages the lifecycles of computing instances in the OpenStack environment. On-demand response includes VM creation, 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

1. OpenStack Overview
2. **Overview of Emerging Technologies**
  - Edge Computing
  - Blockchain
  - Cloud Native

# What Is Edge Computing?

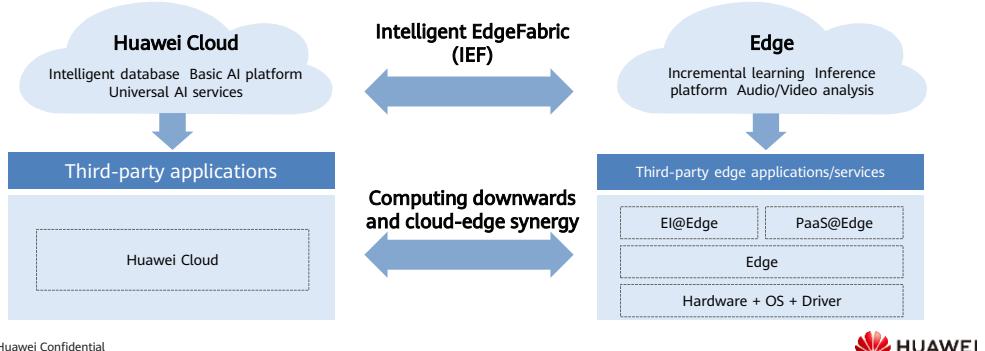
- This computing architecture integrates the network, computing, storage, control, and application on edge nodes to meet user requirements for timeliness, intelligence, data aggregation, and security.



- According to IDC statistics, more than 50 billion terminals and devices would be connected to the Internet by 2020. In the future, more than 50% of data will be analyzed, processed, and stored on the network edge.
- By 2025, there will be about 350 million street lamps around the world, on which billions of cameras and various environment sensors are installed. These cameras and sensors generate hundreds of millions of GB of data every day, which needs to be analyzed, processed, and stored.

## Intelligent Edge

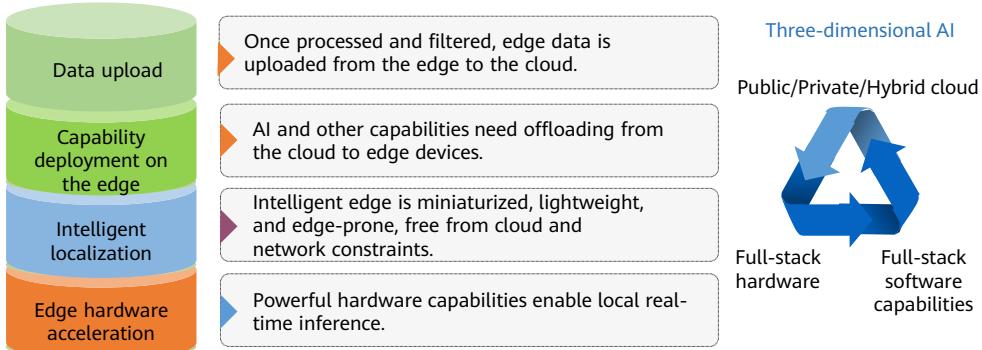
- This evolution moves the cloud AI capabilities down to the edge nodes for local processing.
- Edge computing is both supplements and extends traditional cloud computing architecture, reducing workloads thanks to cloud-edge synergy.
  - Edges connected to the cloud are strong and flexible.
  - Clouds connected to edges houses data diverted and application services



11      Huawei Confidential

- 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.

# Intelligent Edge Features



- 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.

# Contents

1. OpenStack Overview
2. **Overview of Emerging Technologies**
  - Edge Computing
  - Blockchain
  - Cloud Native

## What Is Blockchain?

- Blockchain, also known as distributed ledger technology, is a tamper-proof, non-repudiation accounting mechanism maintained by multiple parities. Used in conjunction with cryptography, it secures transmission and access, and ensures data storage consistency.
- Blocks validated by orderers through cryptography then sequentially form a blockchain (or distributed ledger).
- Blockchain is a low-cost computing and collaboration paradigm used to build trust in an untrustworthy environment. It is vital for developing tomorrow's digital economy and trust system.



- The blockchain technology will be more widely used in the coming years. Considered as a revolutionary and disruptive technology, it can upgrade the existing service progress with its excellent efficiency, reliability, and security.
- Blockchain technology empowers enterprises with the following advantages:
  - Trust is built among parties by reliably sharing data.
  - Decentralized, shared, and permit-required ledgers integrate data into a system to break down data silos.
  - Data is highly secured.
  - Lower dependency is required on third parties.
  - Real-time, tamper-proof records are shared among participants.
  - Authenticity and integrity of products in the business flow are ensured by participants.
  - Products and services in the supply chain are tracked and traced seamlessly.

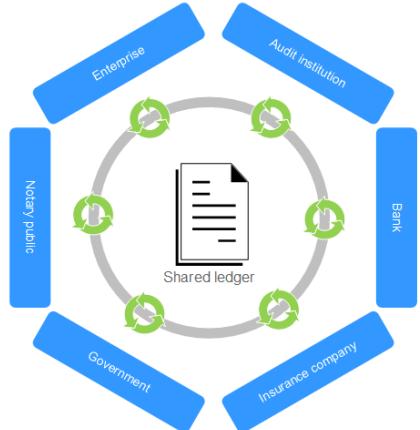
## Blockchain Concepts

- Blockchain is an innovation that combines multiple existing technologies.
- The related technologies include:
  - 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.

- Blockchain combines shared ledgers, consensus algorithms, security and privacy protection, and smart contracts. It features multi-center, consensus and trust, immutability, and traceability. In a blockchain system, all participants share ledgers, which can solve the challenges in traditional business networks.

## Blockchain System Architecture

- Ledgers are shared by participants in a business network and updated upon each transaction.
- Cryptographic algorithms ensure transaction security by limiting participant access only to related ledger content.
- Transaction-related contract clauses are embedded into the transaction database to form smart contracts. These clauses are automatically executed when an event meets clause conditions.
- Consensus algorithms ensure that transactions are validated by all involved parties and meet supervision and audit requirements.



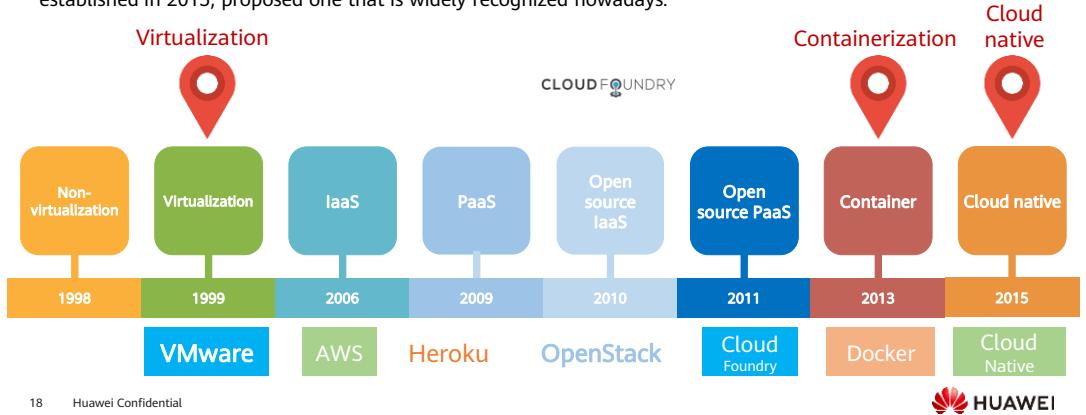
- The application scenarios of blockchain include:
  - Inter-company transactions: Blockchain technology ensures transaction consistency and accounting balance without the need for reconciliation. It supports transactions among different systems and provides traceable and immutable E2E information for internal and external audits.
  - Supply chain logistics: In addition to transparent rules and automatic settlement, blockchain technology enables E2E tracking of goods all the way from production to final reception, improving the trust between consumers and partners in the supply chain. Electronic proofs of delivery (PODs) reduce the delay caused by paper works. Smart contracts enable automatic settlement to improve efficiency.
  - Healthcare: The healthcare consortium blockchain connects information systems of healthcare institutions, so that regional inspection as well as ultrasound and radiological examination results can be securely exchanged for online healthcare, two-way referral, and remote consultation. Encryption and smart contract-based authorization mechanisms offer patients access to their own healthcare data while protecting their privacy. Others can access the data only when authorized.

# Contents

1. OpenStack Overview
2. **Overview of Emerging Technologies**
  - Edge Computing
  - Blockchain
  - Cloud Native

## Cloud Technology Development – Cloud Native

- The concept of cloud native was first put forward by Matt Stine from Pivotal in 2013.
- Matt is a 15-year veteran of the enterprise IT industry, with experience spanning architecture design and consulting. The definition of cloud native kept evolving in the community and Cloud Native Computing Foundation (CNCF), established in 2015, proposed one that is widely recognized nowadays.



18 Huawei Confidential



- In 2015, Pivotal put forward the definition of cloud native, that is, cloud native is an approach to building and running applications that exploits the advantages 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.
  - Cloud computing is the today for IT development and cloud native is the tomorrow. The former lays an architecture foundation for the latter.**
  - Cloud native technologies are witnessing foreseeable, wider implementations and allow organizations to innovate faster.
  - According to Gartner, 70% of global organizations will run three or more containerized applications in production by 2023.

— CNCF



 HUAWEI

- Cloud native involves a large number of PaaS innovations. Deep dives into PaaS are the easiest way to leverage and upgrade cloud computing. CNCF is committed to the standardization of cloud native technologies and provides standard interfaces for users to use cloud services, avoiding vendor lock-in. Cloud native is not only an upgrade for the architecture of the applications that run on the cloud, but also an upgrade for the cloud platforms and cloud services.
- Containerization is a virtualization technology, which is also called operating system level virtualization. This technology virtualizes the operating system kernel and allows user space software instances to be divided into several independent units. These software instances are also called containers.
- Microservices are about the software architecture, based on small building blocks each for a single responsibility and function. Complex, large-scale applications can now run in small modules. Functional blocks communicate with each other using a language-independent/agnostic API set.
- Service mesh decouples service communication from service processes via sidecars, and decouples the data plane from the control plane.
- Immutable infrastructure means an instance of any infrastructure becomes read-only once it is created. If you need to modify or upgrade the instance, you replace it with a new one.
- Declarative APIs describe the desired states of the system to implement deployment and control.

# 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>

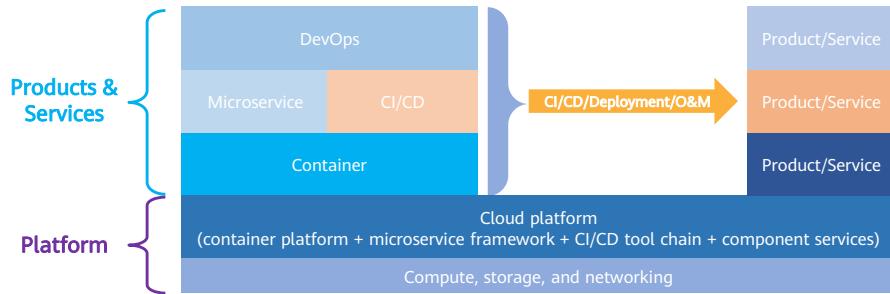
- Cloud-native applications are a collection of **small, independent, and loosely coupled services**. They are designed to deliver well-recognized business value, like the ability to rapidly incorporate user feedback for **continuous improvement**. In short, cloud-native app development is a way to speed 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>

# Comprehensive Understanding of Cloud Native Applications

- **Cloud native** applications are **running on the cloud** to **exploit the advantages of the cloud**.
- Applications are packaged, distributed, and deployed in **containers**. The **microservice architecture** is used by applications to make full use of **cloud component services**. The organization architecture and method of **DevOps** and the **CI/CD** tool chain are jointly used to implement **continuous delivery** of products and services.



- 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.

## 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

- This course has taught you the basic concepts and components of OpenStack, and introduced emerging technologies, including edge computing, blockchain, and cloud native.
- The HCIA cloud computing modules have come to an end. Continue to build on your knowledge with Huawei Cloud Stack solution architecture, resource management, operations, and O&M management.

## 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.

Copyright©2022 Huawei Technologies Co., Ltd.  
All Rights Reserved.

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

