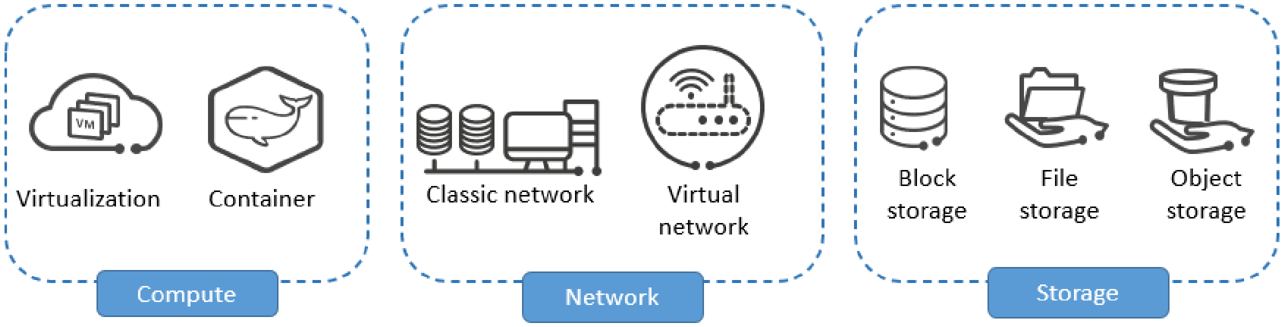
Cloud Computing Technologies

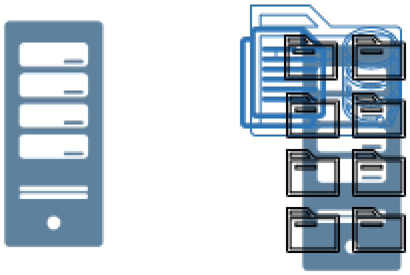


- **Compute services** provide the computing power required for running services such as websites, office software, and data analysis. Currently, typical compute cloud services are VMs and containers.
- **Network services** provide resource connectivity and isolation, such as data center networks and campus networks. On the cloud, VMs use virtual networks (for example, VPC) that have a logical topology similar to that of traditional networks.
- **Storage services** include:
  - **Block storage**: features high performance and low latency, meeting different high I/O service requirements.
  - **File storage**: allows file sharing among multiple servers or enterprise departments.
  - **Object storage**: features a flat, easy scale-out architecture, which is suitable for cloud storage. It is mainly used for massive data storage, cold data backup, and software repository.

Compute

What is Virtualization? The virtualization technology refers to the process of creating multiple VMs that share the hardware resources of a physical server.

- A VM consists of disk files and description files, which are encapsulated in the same folder.
- Multiple VMs running on the server are separately encapsulated in multiple folders and mutually isolated.
- These folders can be stored in the file system provided by the underlying storage. Therefore, multiple VMs can be stored or run on a shared medium.



In computer technologies, virtualization is a resource management technology. It abstracts various physical resources of a computer, such as CPU, memory, disk space, and network adapters, converts the resources, and presents the resources for segmentation and combination into one or more computer configuration environments. In this way, the uncut barriers between physical structures are broken, allowing users to use computer hardware resources in a better way than the original configuration. As shown in the figure, a physical server is divided into multiple files through virtualization, and each file represents a VM.

Virtualization vs. Cloud Computing

- Virtualization is the fundamental technology that powers cloud computing. It transforms physical hardware into virtual resources. On the other hand, the cloud is an environment that delivers virtualized resources on-demand through the Internet.
- Virtualization is a key technology of cloud computing. It aims to abstract physical resources into logical resources for flexible allocation. Virtualization offers scalable, distributed, and HA resources for cloud computing.
- Cloud computing allows users to use cloud resources on demand, relying on the virtualization technology.

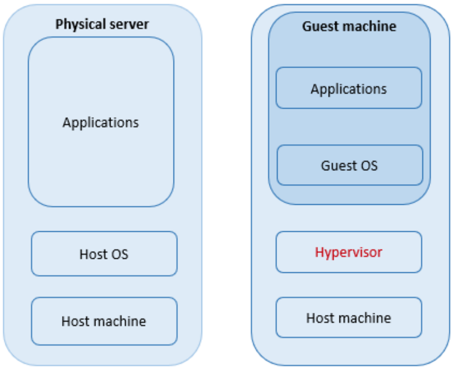
Main Features of Virtualization

- **Partitioning**: Multiple VMs can run on one physical server, which means that the virtualization layer can allocate the resources of a physical server to multiple VMs. This is called partitioning.
- **Isolation**: If one VM on a server is faulty or infected with viruses, the other VMs can still run properly.
- **Encapsulation**: VMs exist in the virtualization system as files. You can migrate VMs by cutting/copying and pasting files.
- **Independence**: After being migrated to another physical server, a VM can properly run without any modification on the server because VM OSs are decoupled from physical hardware.

Important Virtualization Concepts

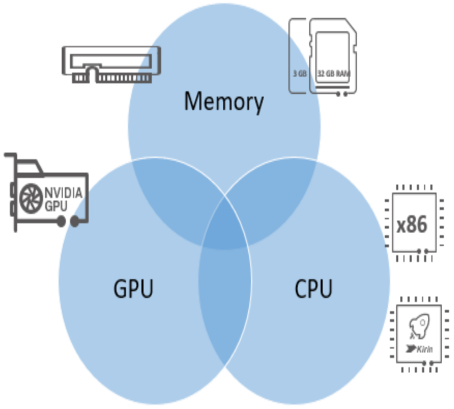
Hypervisor: It is also called virtualization software or VM monitor. Hypervisor is used to create and run VMs on physical servers. The mainstream open-source virtualization technologies are Xen and KVM.

- **Guest OS:** Virtual machine (VM) OS
- **Guest Machine:** VM
- **Hypervisor:** Virtualization software layer/Virtual machine monitor (VMM)
- **Host OS:** OS running on a physical machine
- **Host machine:** Physical machine



Computing Resources Around Us

- Computing essentially refers to the process of obtaining information. In the ICT industry, several resources are needed to calculate data and obtain information.
- A computer system consists of a CPU, memory, disk, and network resources. Compute resources include CPU, GPU, and memory.
- **Central Processing Unit (CPU)** is the computing and control core of a computer system, which processes information and executes programs.
- **Memory** is an important component of a computer system. It is used to store CPU computing data and exchange data between memory and external storage (such as hard disks).



- **Graphics Processing Unit (GPU)** is a microprocessor that performs image computation on PCs, workstations, game consoles, and mobile terminal devices such as tablets and smartphones.

HUAWEI CLOUD Compute Services

- An Elastic Cloud Server (ECS) is a VM on the cloud consisting of vCPUs, memory, OS, and EVS disks. After buying an ECS, you can use it on the cloud just like you would use your local PC or physical server.
- Auto Scaling (AS) automatically scales compute resources based on your demands and the AS policies you have configured, properly adjusting the number of ECSs as the service load changes over time.
- An image is a template used to create servers or disks. Image Management Service (IMS) provides image lifecycle management. With the IMS, you can create a system or data disk image from a server or an external image file. You can also create a full ECS image from an ECS or a backup of an ECS.

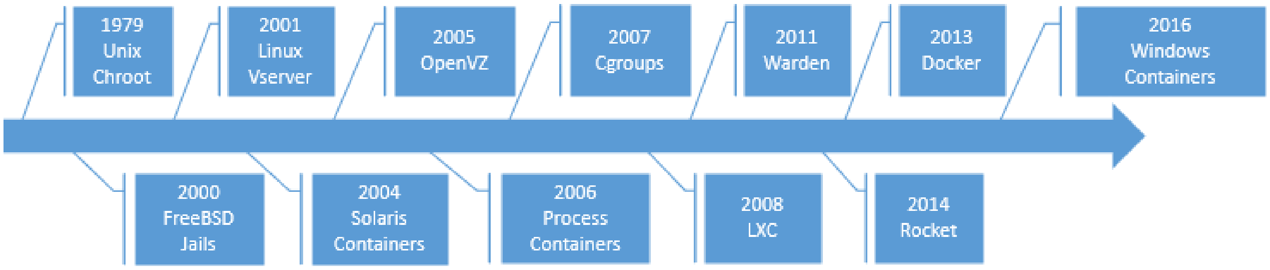
What is a Container? A container is a lightweight, portable technology for application packaging. It is a standard unit that packages an application's code and all its dependencies, enabling the application to run across different computing environments. Simply put, containers are like standardized boxes that can hold different types of things and be put into different cabinets.

Containers can:

- Package software into standardized units for development, migration, and deployment.
- Isolate compute, storage, network, and other resources.
- Start, stop, deploy, and migrate applications agilely and instantly.
- Allow developers to focus on R&D and O&M engineers to focus on system maintenance.

Container Technology Development

- Two challenges in the development of container technology:
  - ➢ Unified platform
  - ➢ Usability

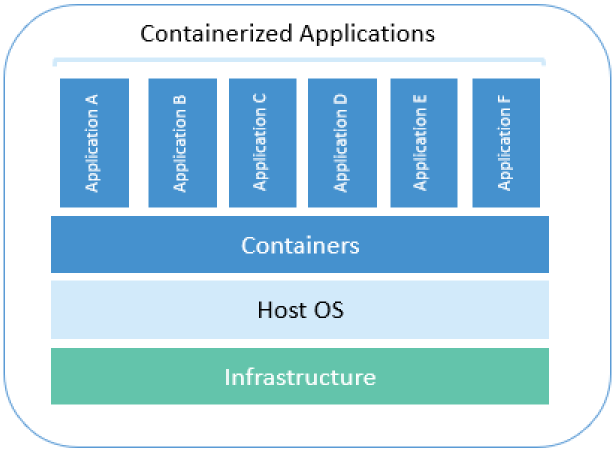


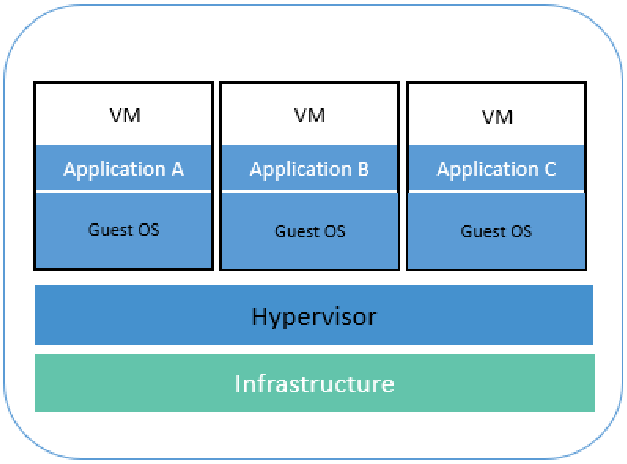
- Container technology was born in 1979 and introduced as the chroot operation in UNIX. Chroot provided an isolated file system for each progress so their root directories can be easily changed. This is the origin of OS virtualization.
- In 2000, BSD released FreeBSD Jails based on chroot. In addition to file system isolation, FreeBSD Jails isolate users, networks, and other resources. An IP address was assigned to each jail, which is an independent, smaller computer system, for independent software installation and configuration.

- In 2005, SWsoft released OpenVZ, which was similar to Solaris Containers. OpenVZ uses a modified Linux kernel to provide virtualization, isolation, resource management, and checkpoints. Since then, kernel virtualization has become a mainstream solution.
- In 2006, Google launched Process Containers. Process Containers, renamed as control groups (cgroups) later, were designed for limiting, accounting, and isolating resource usage (CPU, memory, disk I/O, network) of a collection of processes. In 2007, cgroups were merged into Linux kernel 2.6.24.
- In 2008, LXC (the first, most complete implementation of Linux container manager) was implemented using cgroups and Linux namespaces. LXC can work on a single vanilla Linux kernel without requiring any patches.
- In 2013, Docker was launched. It was initially an internal project of dotCloud, a PaaS company. Just as Warden did, Docker used LXC in its initial stages and later replaced LXC with its own libcontainer. Docker separated itself from the pack by offering an entire ecosystem for container management, including Open Container Initiative, Container Registry, REST API, CLI, and Docker Swarm.
- In 2014, CoreOS introduced the container engine rkt as an alternative to Docker to improve container security. Containers tools related to rkt include the service discovery tool etcd, the networking tool flannel, etc.
- In 2016, Microsoft launched Hyper-V containers in Windows Server. Hyper-V containers are similar to Linux containers and provide isolation for each container so processes in a container are isolated from the outside. It features both the security of VMs and the lightweight of containers.

Difference Between Containers and VMs

- Containers and VMs have similar advantages in resource isolation and allocation but different functions because containers virtualize OSs instead of hardware. Containers are more portable and efficient.
- There is no virtualization layer in the container architecture. Therefore, containerization is called lightweight virtualization. Applications running in containers have better performance than those in VMs.
- Containers have become popular because of many benefits, including:
  - ➢ Agile building and deployment of applications: The creation of container images is easier and more efficient than that of VM images.

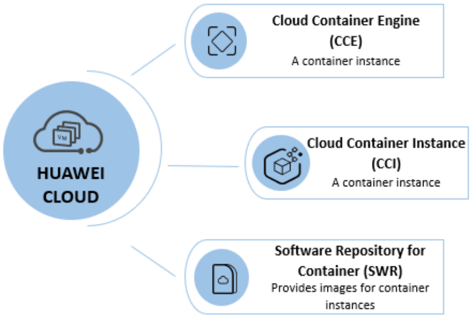




- Consistent development, integration, and deployment: Containers can be quickly restored using images. You can customize new images for consistent container building and deployment.
- Portability across clouds and OSs: Containers can run on Ubuntu, RHEL, CoreOS, Google Kubernetes Engine, physical servers, etc.
- Application-centered management: The abstraction is improved from virtualizing hardware for OS isolation to virtualizing an OS for application isolation.
- Loosely coupled, distributed, elastic, independent microservices: Applications are divided into independent, small units and can be deployed and managed separately instead of running on a single large server.
- Isolated resources: Application performance can be predicted.
- High resource utilization: Resources can be fully used.

- Containers are an abstraction at the application layer. A container packages up code and its dependencies required for the proper running of an application. Multiple containers can run on the same server with a shared OS kernel. Each container runs as an independent process in the user space. Containers take up less space than VMs, process more applications, and require less CPU and memory.
- Virtual Machines (VMs) are an abstraction of physical hardware and turn one server into multiple servers. The hypervisor allows multiple VMs to run on the same physical server. Each VM has its own OS, applications, necessary binaries, and libraries, taking up tens of GB. The startup speed of a VM may be slow.
- **Container image**: A container image is dedicated to running a specific service and usually contains only the resources required for running the service. Many widely used images are tens of MB or less in size.
- **VM image**: A VM image offers the operating environment (including the OS kernel) required by common processes and provides a complete collection of functions. The minimum size of a VM image is hundreds of MB.

HUAWEI CLOUD Container Services


HUAWEI CLOUD
Cloud Container Engine (CCE)
A container instance
Cloud Container Instance (CCI)
A container instance
Software Repository for Container (SWR)
Provides images for container instances

- **Cloud Container Engine (CCE)** is a high-performance, high-reliability service through which enterprises can manage containerized applications. CCE supports native Kubernetes applications and tools, allowing users to easily set up a container runtime environment on the cloud. CCE Turbo clusters run on the cloud native 2.0 infrastructure, accelerating compute, network, and scheduling.
- **Cloud Container Instance (CCI)** is a serverless container engine that allows users to run containers without creating or managing server clusters.
- **SoftWare Repository for Container (SWR)** allows users to easily manage the full lifecycle of container images and facilitates secure deployment of images for your applications. Users can upload, download, and manage container images through SWR Console, community CLI, or SWR APIs.
- SWR can either work with CCE and CCI or be used as an independent container image repository.

Network

Networks bridge devices and VMs and allow them to communicate with each other. Therefore, networks are essential for ICT infrastructure.

Basic Concepts of Conventional Networks

- **Broadcast and unicast**: The communication between two devices is like that between people. The unicast, like one person talking to another, refers to the information that is sent and received between two nodes. The broadcast, like one person using a loudspeaker to talk to many people, has higher communication efficiency and ensures that the information can be sent to all related devices.
- **Router**: A router is a hardware device that connects two or more networks. It works as a gateway to read the address of each data packet and decide how to forward it.
- **Default gateway**: To understand the default gateway, we need to know what a gateway is. A gateway is a device that connects a subnet to an external network. When a device sends information to a host, a subnet mask determines whether the destination host is on the local subnet according to the destination address. If the host is on the local subnet, the device can directly send information to the host. If not, the device will first send the information to the default gateway or router, which then forwards the information to other networks to reach the host.
- **Virtual Local Area Network (VLAN)**: VLAN is a group of logical devices and users, which are organized based on functions, departments, and applications, regardless of their physical locations. Such devices and users communicate with each other as if they are on the same network segment. VLANs can be used to isolate different services.

What Does a Router Do? Our PCs can access the Internet through a router. Likewise, servers can be connected to the Internet by using a router. A **router** is a gateway device that operates on the third layer of the OSI Model, the network layer. It stores and forwards packets between different networks and routes data from one subnet to another. In network communications, routers can determine network addresses and select IP routes. Routers can flexibly set up connections for networks and send packets between them through different media access control mechanisms. Routers accept information only from the source and other related routers, functioning as interconnection devices on the network layer.

What Does a Layer 2 Switch Do? A network switch is used to forward electrical signals, and establishes an exclusive electrical signal route for any two nodes connected to the switch. Ethernet switches are most commonly used. Other common switches include telephone voice switches and fiber switches. Switching allows devices to automatically or allows you to manually send information to an appropriate route, meeting the requirements of both communications ends. A switch has multiple ports, with each port providing the bridging function. A port can be connected to a local area network (LAN) or a high-performance server or workstation. On a conventional network, Layer 2 switches use VLANs to isolate network planes.

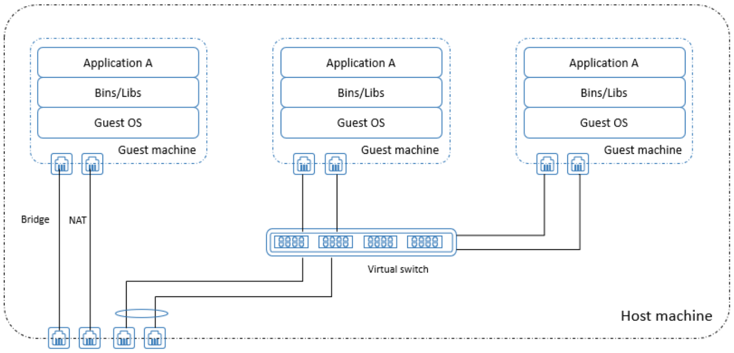
What Does a Layer 3 Switch Do? For safety and management purposes, a large local area network (LAN) must be divided into several small LANs to reduce the impact of broadcast storms, so the virtual local area network (VLAN) technology is widely used. Communications between different VLANs are forwarded by routers. With the increase of access across networks, if only routers are used, the network scale and access speed are restricted because there is a limited port quantity and the routing speed is slow. To address this, Layer 3 switches are developed. Layer 3 switches are designed for IP addresses. These switches provide simple APIs and are strong in processing Layer 2 packets, suitable for routing and switching data in large LANs. Layer 3 switches not only replace or partially complete the function of traditional routers in the third layer of the network model but also have almost the same switching speed as the second layer. And the price of Layer 3 switches is cheaper.

What Does a NIC Do? NICs are mainly used to connect different devices. Like a telephone card, they ensure devices can communicate. In addition, NICs can be bound to deliver higher reliability and better network performance.

- The onboard NIC provides network expansion capabilities. It transmits data from servers to other devices, providing application services externally.
- Commonly supported NIC speed rates include 100 Mbit/s, 1 Gbit/s, and 10 Gbit/s.

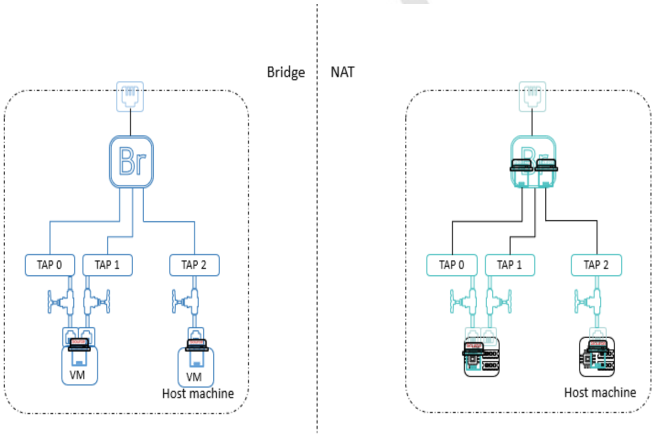
Basic Concepts of Virtual Networks

- Why is a virtual network required? VMs hosted on a physical machine may be in different IP address ranges, so these IP address ranges need to be isolated. In addition, VMs need to share the same physical NIC to access external networks. Therefore, virtual switches are used on servers to construct virtual networks.
- In network virtualization, the first problem to be solved is how to map the virtual NICs of the VMs to the physical NICs of the physical server where the VMs are hosted. As shown in the figure, we can use network bridges, NAT and virtual switches to solve this problem.



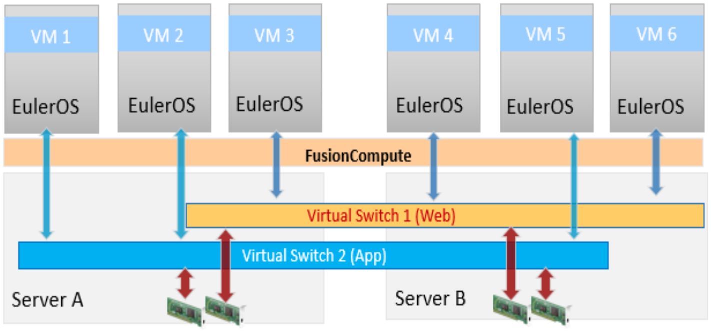
What Do Bridge and NAT Do?

- Both a bridge and NAT can forward the traffic of different VMs to physical NICs so that data packets can be routed from the server to the physical switch, implementing the communication between VMs and between VMs and external networks.
- Virtual switches also have the bridging function. A virtual switch has a table that defines mapping between MAC addresses and ports to isolate collision domains. Simply speaking, a bridge connects different physical LANs at the data link layer.
- NAT forwards the traffic to external networks through translating network addresses. NAT not only avoids the lack of IP addresses, but also protects computers on the private network from being attacked by other networks.



What Does a Virtual Switch Do? Like the bridge and NAT, virtual switches are used to transmit the internal traffic of VMs to the external network through the network port of the physical server where the VMs reside. The common virtual switch models include OVS and EVS.

- **Open vSwitch (OVS)**: An OVS is a software-based open-source virtual switch. It supports multiple standards and protocols with additional support for the OpenFlow protocol, and can be integrated with multiple open-source virtualization platforms. An OVS can be used to transmit traffic between VMs and implement communication between VMs and external networks.
- **Enhanced vSwitch (EVS)**: An EVS is an enhanced OpenFlow-compliant virtual switch that improves the I/O performance based on the OVS forwarding technology. I/O performance is significantly improved by using the Intel DPDK technology and using user-mode processes rather than NICs to send and receive data.
- On an OVS, data is received and sent in the kernel mode, but on an EVS, data is processed in the user mode.
- **Distributed Virtual Switch (DVS)**: Same as a physical switch does, a DVS constructs the network between VMs and connects VMs to external networks.
- A virtual NIC of a VM communicates with an external network by connecting to the DVS and then by connecting to the physical NIC of the host through the DVS uplink.
- Compared with traditional switches, using virtual switches reduces network devices and simplifies the network architecture, relieving the pressure of system management and maintenance.



HUAWEI CLOUD Network Services

- A Virtual Private Cloud (VPC) is a private and isolated virtual network on HUAWEI CLOUD. Users can configure IP address ranges, subnets, and security groups, assign EIPs, and allocate bandwidths in a VPC.
- Public NAT gateways and private NAT gateways are used in different scenarios to provide the network address translation. A public NAT gateway provides SNAT and DNAT so that cloud servers in a VPC can share EIPs to access the Internet. A private NAT gateway provides the network address translation for servers in a VPC.
- The EIP service provides independent public IP addresses and bandwidth for Internet access. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, load balancers, and NAT gateways. This service provides various billing modes to meet diverse service requirements and allows cloud servers in a VPC to share the same private IP address to access or provide services accessible from an on-premises data center or a remote VPC.

Storage

How Does Cloud Storage Work? A storage medium is any technology -- including devices and materials -- used to place, keep and retrieve electronic data. In terms of data storage, the existing cloud storage products can achieve higher efficiency at lower cost. Therefore, cloud storage will be an inevitable choice for individuals and enterprises.

Mainstream Storage Types

Traditional servers have computing and storage coupled and use their local physical disks to store data. This is what we call the traditional block storage, where a disk is connected to a server through a bus, delivering low latency. However, the number of disks attached to the server is limited, so traditional servers have poor performance in capacity, bandwidth, and reliability. The explosive data growth poses high requirements on data reliability, which requires decoupled compute and storage. To address this, storage arrays appear. Traditional disk arrays comprise controllers and disk enclosures. Two or more controllers can be used to provide high reliability. By adding disk enclosures, the capacity of disk arrays can be hundreds of thousands of times larger than that of local disks. Disk arrays independently connect to servers through FC switches or IP switches. This is today's block storage.

- As the IT system further develops, enterprises want their files to be shared among multiple hosts for concurrent access. This is shared file storage. Shared file storage shares data in the same data center or equipment room.
- As more and more Internet applications need to access data over the Internet using terminal devices, object storage that supports HTTP and HTTPS protocols is widely used. Object storage allows applications to access data by calling APIs and adopts a distributed architecture featuring large capacity and high reliability.

Block Storage

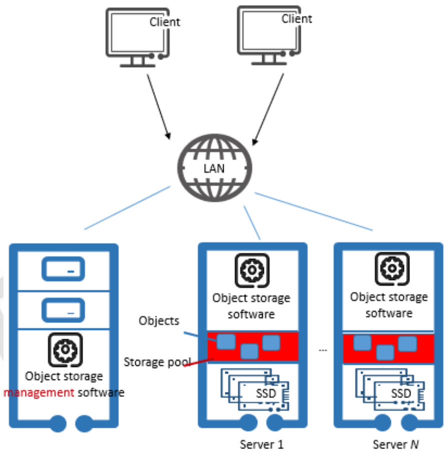
- Block storage cannot be directly used in an operating system. Before using a block device, you must format it and create a file system on it. Data in the operating system is stored as files.
- Block storage has the lowest latency among the three types of storage and is ideal for mission-critical applications such as databases and ERP systems.

File Storage

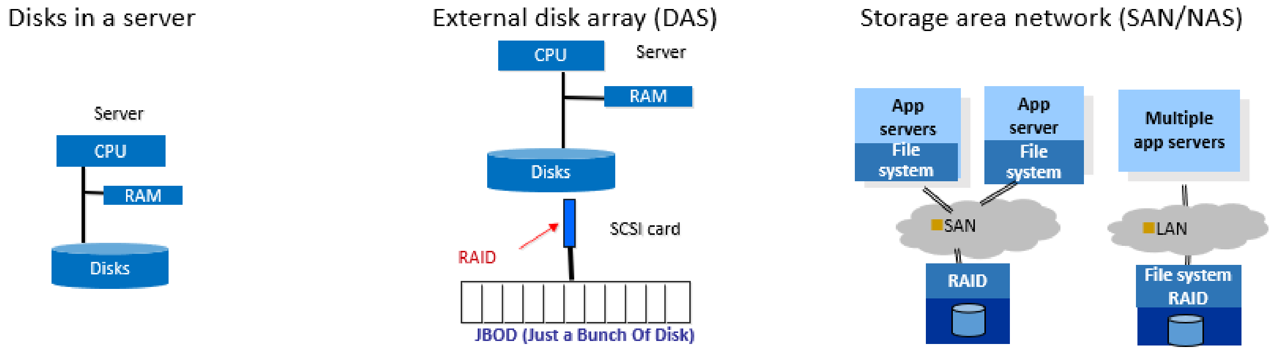
- **Network File System (NFS)**: NFS is a file-sharing protocol between UNIX operating systems. It commonly applies to Linux clients.
- **Common Internet File System (CIFS)**: CIFS is a protocol that allows programs to access files on remote computers over the Internet. It mainly applies to Windows clients.
- File storage provides petabyte (PB)-level capacity and ms-level latency and is perfect for scenarios where data needs to be shared among multiple compute nodes, such as HPC and office automation.

Object Storage

- Object storage has large-scale data management capability, which is its biggest advantage over file storage. File Storage uses a hierarchical structure to manage all files and directories. If there are too many files or directories stored, the search performance will be greatly reduced. Object storage provides a flat structure where all objects are stored at the same logical layer. This keeps the object search speed almost unchanged even if there are tens of billions of objects. However, object storage uses application-level APIs instead of system-level APIs. Traditional applications need to be redeveloped when being migrated to object storage systems, which makes the popularization of object storage difficult.
- Object storage is applicable to scenarios such as big data, IoT, backup, and archive. It provides EB-level capacity and has the highest data durability among the three types of storage.



Enterprise Storage



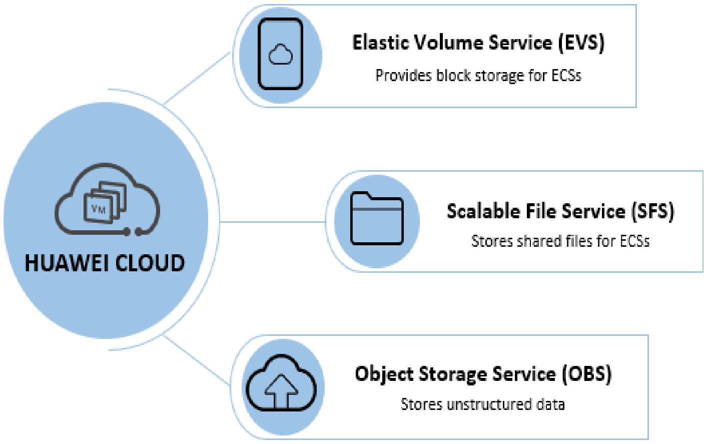
- **Direct Attached Storage (DAS)** connects an external storage device to an application server through the SCSI or FC interface, making the storage device part of the server. In this case, the data and operating system are not separated.
- **Network Attached Storage (NAS)** uses TCP/IP, ATM, and FDDI to connect storage devices, switches, and clients, and all these components form a private storage network. NAS integrates storage devices, network interfaces and Ethernet technology and stores data directly over Ethernet, which separates the storage function from the file server.
- **Storage Area Network (SAN)** is a private storage network that connects storage arrays and servers through switches.

Distributed Storage: Distrubuted storage systems virtualize the available storage resources across all hosts of an enterprise to a virtual storage device. This way, data is stored in different locations on the storage network, improving system reliability, availability, and access efficiency.

- As data grows exponentially, storage of massive amount of data imposes great pressure on local storage and brings heavy burden to existing storage systems. To relieve the pressure, we have to adopt distributed storage and distributed file systems.
- How can we ensure high performance and high availability of distributed storage?
- In addition to the backup, active-active, and multi-active architectures in the traditional architecture, multiple data copies are stored in the system to ensure high reliability and availability of the distributed storage system. If a storage node becomes faulty, the system can automatically switch the node's service to other nodes, achieving automatic fault tolerance. The distributed storage system leverages replication protocols to synchronize data to multiple storage nodes and ensures data consistency between copies. A piece of data has multiple copies, among which there is only one primary copy, and the rest are backup copies. Consistency is used to ensure data integrity when data is replicated from the primary copy to backup copies.

HUAWEI CLOUD Storage Services

- **Elastic Volume Service (EVS)** provides persistent block storage for ECSs and BMSs. With data redundancy and cache acceleration techniques, EVS offers high availability, strong durability, and low latency. Users can format an EVS disk, create a file system on it, and store data persistently.
- **Scalable File Service (SFS)** is a network attached storage (NAS) service that provides scalable, high-performance file storage. With SFS, you can enjoy shared file access spanning ECSs, BMSs, and containers created on CCE and Cloud Container Instance (CCI).


HUAWEI CLOUD
VM
Elastic Volume Service (EVS)
Provides block storage for ECSs
Scalable File Service (SFS)
Stores shared files for ECSs
Object Storage Service (OBS)
Stores unstructured data

- **Object Storage Service (OBS)** provides a stable, secure cloud storage that is scalable, efficient, and easy to use. It offers REST APIs and allows users to store any amount of unstructured data in any format.