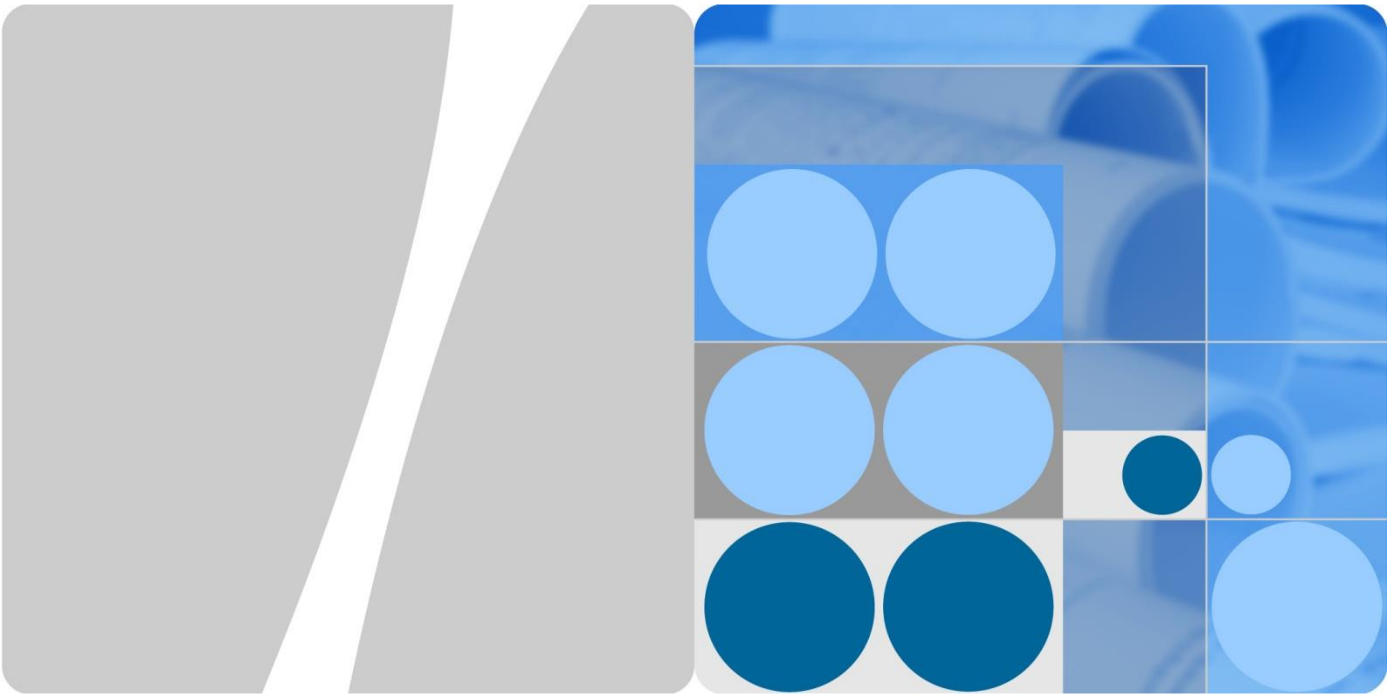


Huawei FusionSphere 6.3.1

Feature Description (Virtualization Suite)

Issue 1.1

Date 2018-09-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

Contents

1 FusionSphere Virtualization Suite

1.1 Computing Virtualization

1.1.1 FSFD-010101 VM QoS

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

VM QoS allows users to control the quality of service (QoS) for computing resources (such as CPUs and memory) in a flexible manner.

Benefits

This feature implements measurement of computing capabilities and limits the computing capabilities of VMs to a specific range. With this feature enabled, VMs requiring different computing capabilities do not affect each other. This feature also optimizes allocation of computing resources and resource reuse, thereby reducing the cost and improving user satisfaction.

Description

- CPU QoS

  CPU QoS ensures optimal allocation of computing resources for VMs and prevents resource contention between VMs due to different service requirements. Therefore, CPU QoS can effectively increase resource utilization and reduce costs.

  CPU QoS values can be set during VM creation based on the planned VM services. CPU QoS determines VM computing capabilities. The system ensures the VM CPU QoS by setting the minimum computing capability and the computing capability upper limit for VMs.

- Memory QoS

  Memory QoS allows VM memory to be intelligently allocated based on the preset percentage of reserved memory. Memory overcommitment technologies, such as memory ballooning, are used to provide more virtual memory resources, thereby increasing memory utilization. In this case, memory QoS is used to reserve the minimum memory for reliable running of VMs and thereby ensures optimal use of memory.

Users can set the reserved memory percentage based on service requirements. The main principle of memory overcommitment is to first use the physical memory.

Enhancement

None

1.1.2 FSFD-010102 VM Time Synchronization

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition or above.

Summary

VM Time Synchronization allows VMs to synchronize time from the host.

Benefits

This feature simplifies time configuration for VMs.

Description

FusionSphere supports two time synchronization modes, the free mode and force mode.

In free mode, users can adjust the VM system time, ranging from the year 2000 to 2037, and the time will be kept.

After this feature is enabled for a VM, the VM synchronizes the time from the host every minute to ensure time consistency. This feature can take the place of simple functions of a Network Time Protocol (NTP) server.

The free mode is the default mode, and the mode to be used can be changed in VM configurations.

Enhancement

None

1.1.3 FSFD-010103 Memory Overcommitment

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Memory Overcommitment allows a server to provide larger virtual memory than its available physical memory.

Benefits

This feature prolongs the memory service time on a physical server by improving memory utilization and therefore reduces the memory procurement cost for customers.

Description

This feature employs the following memory overcommitment technologies:

- Memory ballooning: FusionCompute dynamically reclaims the free memory of a VM and allocates it to other VMs. Applications on VMs are not aware of memory reclamations and reallocations. Memory ballooning does not allow the total VM memory in use on a server to exceed the physical memory size of the server.
- Memory swapping: The system swaps out the content on the reserved VM memory to an external storage file to free the reserved memory and retrieves the content when required.
- Zero page sharing: The system directs all zero data pages on VMs to the same memory page and allocates a new page for a VM only when new data is written to the VM.

The recommended memory overcommitment ratio is less than 120%. Do not enable memory overcommitment for the servers that have greater than 80 physical CPU cores and 64 GB of memory.

Do not enable memory overcommitment for the VMs whose memory usage keeps up to 40%.

Enhancement

None

1.1.4 FSFD-010104 CPU Overcommitment

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

CPU Overcommitment allows the system to allocate CPU resources to VMs as required to efficiently utilize CPU resources.

Benefits

With this feature, the system can meet VM resource requirements and efficiently use these resources when the CPU workload is low, thereby reducing costs.

Description

You can configure a CPU reservation value so that CPU resources are allocated to VMs as required. This enables the system to efficiently reuse the CPU resources, and VMs with the CPU reservation value configured are preferentially allocated with required compute resources. This feature enables carriers or enterprises to reduce costs and improve user satisfaction.

In the FusionSphere OpenStack+FusionCompute scenario, you can configure the vCPU overcommitment ratio of a cluster in FusionSphere Cloud Provisioning Service to expand the CPU resources available to the cluster. In this way, more VMs can be created in this cluster. This feature can work with CPU reservation and CPU usage in time-division mode to implement the optimal CPU resource utilization.

Enhancement

None

1.1.5 FSFD-010105 VM Support for UEFI Firmware

Availability

This feature was first available in FusionSphere 5.1 and requires a license of the virtualization suite standard edition or above.

Summary

This feature allows users to configure the GUID Partition Table (GPT) of Unified Extensible Firmware Interface (UEFI) to support system volumes with greater than 2 TB of capacity.

Benefits

This feature allows users to migrate system volumes with greater than 2 TB of capacity from physical servers to the virtualization platform in P2V scenarios.

Description

VMs upgraded from earlier versions to FusionSphere 5.1 support both UEFI and BIOS boot modes but they boot firmware in BIOS mode by default. Users can log in to the system web client to change the boot mode to UEFI secure boot for such as a VM, but the VM may fail to identify its OS. In this case, mount an ISO image to the VM to reinstall the VM OS.

Enhancement

None

1.1.6 FSFD-010106 VM Resource Adjustment

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

VM Resource Adjustment allows users to modify VM specifications to meet service requirements. The VM specifications include the numbers of CPUs and NICs, memory size, and disk size.

The system allows users to modify CPUs and memory sizes for a running VM. New settings take effect upon the next VM startup. Certain OSs also allow the settings to take effect immediately.

Benefits

This feature allows users to modify VM specifications if the current VM specifications do not meet service requirements.

Description

This feature provides the following functions:

- Modifying VM CPU specifications

  Users can modify CPU specifications if the current VM CPUs cannot handle the service load.

- Modifying memory specifications

  Users can modify memory specifications if the current VM memory cannot handle the service load.

- Modifying disks

  Users can add or delete VM disks based on service load.

  Users can attach virtual disks to a running or stopped VM.

  Users can detach unwanted virtual disks from a stopped VM to release storage resources, allowing these resources to be allocated to other VMs.

- Adjusting NICs

  Users can add or delete virtual NICs from a stopped VM to dynamically meet service requirements on NICs. A VM can support one to eight NICs.

  For details about the compatibility of VM hot add, see *FusionSphere SIA 1.3.10.270 Compatibility List 01*. The link of obtaining this document is as follows:

  http://support.huawei.com/carrier/docview!docview?detailId=PBI1-21579393&path=PBI1-21430725/PBI1-21430806/PBI1-21431666/PBI1-21462737/PBI1-19916941/PBI1-19918232/PBI1-21579393/PBI1-22593452&nid=DOC1000400407

Enhancement

None

1.1.7 FSFD-010201 VM Life Cycle Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

VM Life Cycle Management allows users to perform the following operations based on service load:

- Create or delete a VM.
- Start, stop, or restart a VM.
- Hibernate or wake up a VM.
- Manage VM groups.

Benefits

This feature provides basic operation and management functions for VMs, thereby facilitating VM use and management.

Description

Create a VM: Users can create a guest operating system (OS) using a VM template or image, and allocate resources for the OS, thereby creating a VM. After a VM is created, it is in the stopped state and occupies no system resources in this state.

Delete a VM: After a VM is deleted, the system reclaims all the resources occupied by the VM.

Start, stop, or restart a VM: These operations are basic management functions for a VM, and are like using a physical machine.

Hibernate a VM: After a VM is hibernated, the VM is paused and the memory data on the VM is written on the storage device. The VM in the hibernated state does not occupy any CPU or memory resources.

Wake up a VM: Users can resume a VM from the hibernated state by waking it up. After a VM is woken up, the memory data written on the storage device returns to the memory and the VM can resume to run.

Manage VM groups: Users can manage VMs hierarchically using VM folders, which facilitates VM search and simplifies operations to perform on VMs.

Enhancement

None

1.1.8 FSFD-010202 VM Migration

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

VM Migration enables a running VM to be migrated without service interruption to another host that uses the same shared storage as the source host.

Benefits

This feature enables the system to migrate VMs on multiple light-load hosts to a small number of hosts and power off the idle hosts, thereby reducing the power consumed by the data center.

Description

This feature allows users to migrate VMs running on a server to another one before maintaining a host, preventing service interruption.

This feature also allows users to migrate VMs running on a busy host to an idle one, thereby balancing the service load and improving user experience.

Enhancement

None

1.1.9 FSFD-010203 Cross-CPU VM Live Migration

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Cross-CPU VM Live Migration allows VMs to be live migrated between hosts that use different CPUs, thereby improving system compatibility.

Benefits

The hardware devices that compose a virtualization cluster may be purchased at different times and use CPUs of different generations. With the Cross-CPU VM Live Migration feature, VMs are allowed to be live migrated between hosts that use CPUs of different generations.

Description

This feature masks the unique advanced features of the host CPUs and provides the same CPU features to all hosts in a cluster. Therefore, VMs can be migrated to any host in the cluster, but they cannot use the masked advanced CPU features of the host.

CPU features are defined by CPU vendors and are considered to be performance baselines. The FusionSphere system supports only Intel CPUs of the following generations (listed in ascending order of performance baseline): Merom, Penryn, Nehalem, Westmere, and Sandy Bridge. A later CPU generation is compatible with the performance baselines of all earlier CPU generations.

Enhancement

None

1.1.10 FSFD-010204 Shared Nothing VM Live Migration

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite standard edition or above.

Summary

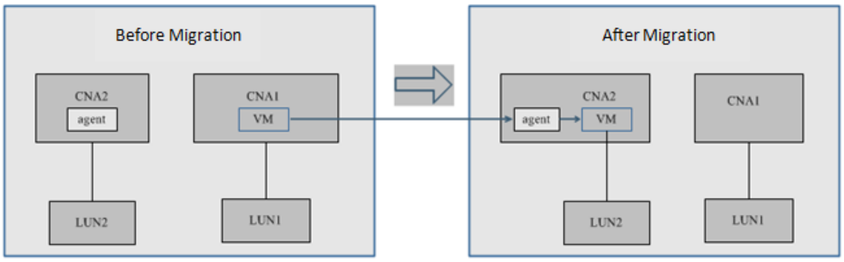
Shared Nothing VM Live Migration enables a running VM with direct-attached storage to be live migrated to another host with direct-attached storage.

Benefits

This feature allows VMs to be live migrated between hosts that use different storage media.

Description

The following figure shows the working mechanism of this feature. In this example, the VM on CNA1 is migrated to CNA2 in the same cluster, and CNA1 and CNA2 each have individual storage logical unit numbers (LUNs). In the migration process, the agent process is used for disk file migration, and the memory migration is the same as that of a common VM live migration.



This feature has the following constraints:

- This feature supports only virtual storage.
- Linked clones do not support this feature.
- VMs with shared disks attached do not support this feature.

Enhancement

None

1.1.11 FSFD-010205 VM Cloning

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

VM Cloning allows users to quickly create a VM by cloning an existing VM. The new VM has the same specifications and storage content as the source VM.

Benefits

This feature allows users to create a VM from an existing one without installing the OS and software.

Description

This feature allows users to clone a VM, including its specifications and user data. This feature simplifies operations and applies to scenarios where several VMs need to be created from an existing one. During the cloning process, the source VM can be stopped or running.

Enhancement

None

1.1.12 FSFD-010206 VNC Login to a VM

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

FusionSphere supports Virtual Network Computing (VNC) login to a VM for troubleshooting in the event that a user fails to log in to the VM.

Benefits

This feature allows a user to remotely log in to a VM to facilitate VM management and maintenance.

Description

VNC Login to a VM allows VMs to be remotely logged in to and controlled from a computer on the same network.

Enhancement

None

1.1.13 FSFD-010207 VM Group Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Different types of VMs are logically divided into different groups (in the format of folders) for efficient management and O&M.

Description

Different types of VMs are logically divided into different groups (in the format of folders) for efficient management and O&M.

Enhancement

None

1.1.14 FSFD-010301 VM Template Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

VM Template Management allows users to manage VM templates, including:

- Create or delete a template.
- Modify a template.
- Create a VM using a template.

Benefits

This feature facilitates VM deployment and creation.

Description

This feature allows system administrators to customize a VM template of specified specifications to create VMs.

A VM template contains the following attributes: template name, image, number of CPUs, memory size, system disk size, number of network interface cards (NICs), QoS, and description.

Enhancement

None

1.1.15 FSFD-010401 Guest NUMA

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Non-uniform memory access (NUMA) nodes are introduced in physical servers to improve the memory access efficiency of CPUs. The CPUs and memory resources used by VMs (guests) are grouped into NUMA nodes based on the memory access efficiencies of the CPUs. A CPU can achieve its maximum memory access efficiency when accessing memory within its own NUMA node.

However, if any VM OS or application requires a second NUMA node, the overall performance of the VM will deteriorate. In this case, Guest NUMA, an enhanced NUMA feature, enables a VM to preferably use memory resources on one NUMA node, thereby improving memory performance.

Benefits

Guest NUMA optimizes memory access efficiency and improves memory performance for VMs. With this feature enabled, CPUs preferably use memory resources on one NUMA node, thereby reducing memory access latency and improving memory performance.

Description

Guest NUMA provides the following functions:

- Topology view: Based on the physical NUMA architecture and VM specifications, an automatically balanced or custom NUMA topology view is presented to VMs. VM OSs and applications access memory resources based on the topology view.
- Initial deployment: The system associates VMs with NUMA nodes based on the VM specifications and workload on the NUMA nodes. VM CPUs and VM memory that belong to the same NUMA node are deployed on the same physical server.

Enhancement

None

1.1.16 FSFD-010402 Host NUMA

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Non-uniform memory access (NUMA) nodes are introduced in physical servers to improve the memory access efficiency of CPUs. Memory is divided into multiple NUMA nodes based on the access efficiency. The performance of a VM that accesses one NUMA node exceeds the performance of a VM that accesses multiple nodes.

The Host NUMA feature automatically allocates the CPU and memory resources of a VM to the same node and balances CPU workload among nodes.

Benefits

This feature ensures that a VM has access to local physical memory in order to reduce memory access latency and improve VM performance. The scale of the performance improvement is determined by the VM memory size and access frequency.

Description

This feature provides the following functions:

- Initial deployment

  When a VM is being started, Host NUMA deploys the VM on a light-load node based on the host memory and CPU load. The VM CPU and memory resources are allocated on the same node.

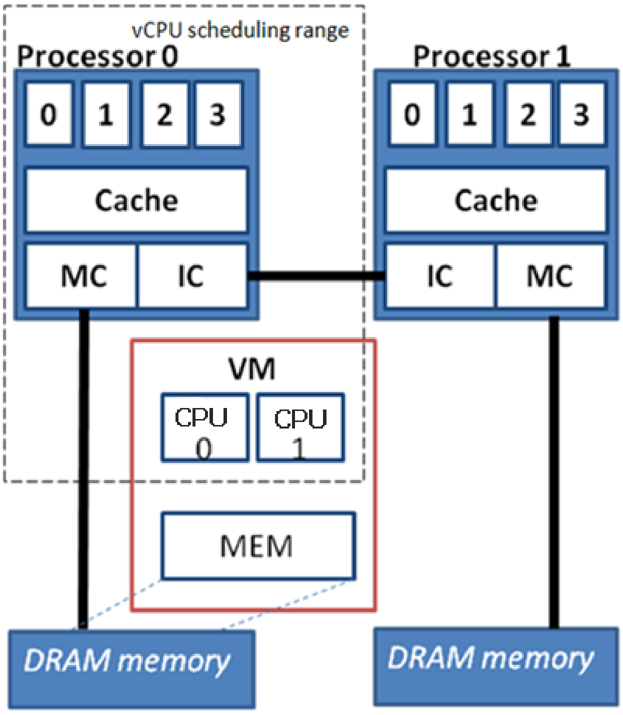
- CPU load balancing

  The CPU load of the node on which the VM is allocated changes as the VM CPU load dynamically changes. Therefore, the CPU resources on one node may be insufficient, while another node may have idle CPU resources. In this case, Host NUMA enables the VMs running on the node with insufficient CPU resources to obtain CPU resources from the node with sufficient resources.

  In this manner, the system dynamically balances the CPU load among nodes. This function eliminates VM performance bottlenecks caused by insufficient CPU resources on a node.

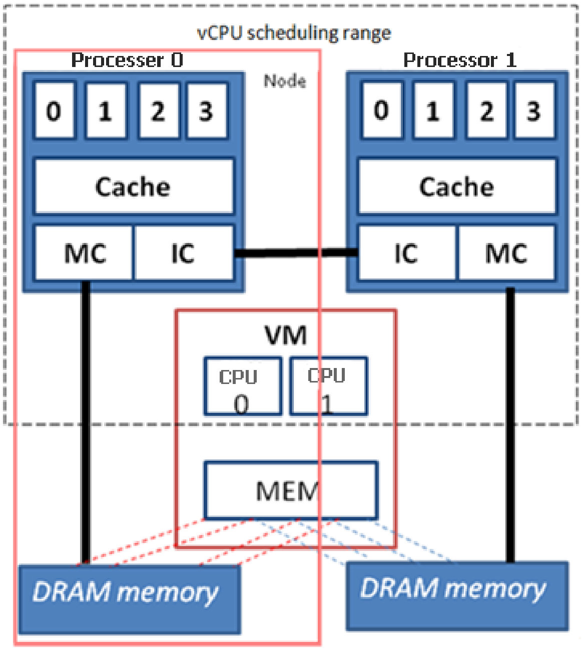
The working mechanism of the Host NUMA feature is as follows:

The system deploys the physical memory of a VM on a node and limits the vCPU scheduling range of the VM to the physical CPU of the node, as shown in the following figure.



Upon VM startup, the system starts the VM on a light-load node and binds the vCPU affinity of the VM to the physical CPUs of the node so that the VM can obtain both CPU and memory resources from the same node. Real-time vCPU affinity binding enables the computing resources to be switched between nodes, thereby implementing CPU load balancing.

To ensure memory performance in case the number of vCPUs on a VM exceeds the number of physical CPU cores on the node, Host NUMA enables the system to evenly deploy VM memory on each node and limits the vCPU scheduling range to the physical CPUs of all nodes, as shown in the following figure.



Host NUMA deploys VMs based on the vCPU affinity settings. If the vCPU affinity is bound to the physical CPUs of one node, the system selects the same node to provide memory and CPU resources for the VMs. If the vCPU affinity is bound to the physical CPUs of multiple nodes, Host NUMA enables the system to provide an equal amount of memory from each node to deploy on VMs. Therefore, VMs can be allocated vCPU resources from the physical CPUs of multiple nodes.

Enhancement

None

1.1.17 FSFD-010501 Dynamic Resource Scheduling

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

Dynamic Resource Scheduling (DRS) enables the system to flexibly schedule resources and achieve load balancing using the intelligent algorithm based on the system load, thereby providing enhanced user experience.

Benefits

This feature dynamically schedules computing resources in a cluster, thereby balancing resource allocation.

Description

DRS policies define scheduling thresholds and periods during which the policies take effect for a cluster. During the set period, if the CPU or memory load on a host exceeds the scheduling threshold, the system migrates some VMs to other light-load hosts to balance the load.

This feature is not supported by the VMs with greater than 4 GB of memory.

Enhancement

None

1.1.18 FSFD-010502 Dynamic Power Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

Dynamic Power Management (DPM) allows the system to power on or off hosts based on service load in clusters to reduce power consumption.

Benefits

This feature helps the system reduce power consumption.

Description

DPM can be enabled only after DRS is enabled.

The DPM policy defines the periods during which the policy takes effect (in hours). During the set period, if the idle CPU or memory rate of a host exceeds the reservation threshold, the system migrates VMs to consolidate host resources and powers off idle servers to save energy. When VMs require more resources, the system dynamically powers on available hosts to provide sufficient resources for the VMs.

Enhancement

None

1.1.19 FSFD-010503 VM Deployment Group

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

VM Deployment Group supports specified rules which determine whether the VMs can run on (or migrate to) specified hosts.

Benefits

Users need specify VMs that must run on the same host or different hosts or VMs that run on or migrate between certain hosts.

Description

This feature provides the following rules:

- **Keep VMs together**: VMs that are added to this rule must run on the same host. One VM can be added to only one **Keep VMs together** rule.
- **Mutually exclusive VMs**: VMs that are added to this rule must run on the different hosts. One VM can be added to only one **Mutually exclusive** rule.
- **VMs to hosts**: This rule associates a VM group with a host group so that VMs in the VM group can only be migrated to hosts in the host group.

Enhancement

None

1.1.20 FSFD-010601 Consistency Snapshot

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

Consistency Snapshot adopts the Microsoft Volume Shadow Copy Service (VSS) to implement data consistency for snapshots.

Benefits

This feature ensures data consistency for certain Windows services.

Description

This feature supports only certain Windows OSs because this feature is based on the Microsoft VSS. Microsoft VSS coordinates with service applications, backup applications, and storage hardware to allow storage devices (such as disks and arrays) to create high-fidelity, time-point-based disk images.

Enhancement

None

1.1.21 FSFD-010602 VM Memory Snapshot

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

VM Memory Snapshot allows users to create snapshots for both memory and disk data of running VMs. The created snapshot can be used to restore both memory and disk information.

Benefits

This feature enables users to restore the system to the status when the snapshot was taken.

Description

VM Memory Snapshot allows users to create snapshots for both memory and disk data of running VMs. The created snapshot can be used to restore both memory and disk information.

Enhancement

None

1.1.22 FSFD-010603 VM Disk Snapshot

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

VM Disk Snapshot allows users to create snapshots for VM disks. These snapshots can be used to restore disk information of the VMs to the status when they were taken.

Benefits

This feature allows users to create disk snapshots and store disk information for stopped VMs.

Description

With this feature enabled, users can create snapshots for disks on stopped VMs to store the disk information at that point in time.

Enhancement

None

1.1.23 FSFD-010701 CD/DVD-ROM Drive

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

This feature provides a virtual CD/DVD-ROM drive for each VM so that ISO images or CD/DVD-ROM devices can be mounted to VMs.

Benefits

This feature allows users to install software on VMs in remote mounting mode.

Description

This feature supports the following mounting modes:

- Shared mode: applies to all OSs, supports only ISO images, and requires complicated operations.
- Local mode: applies to certain OSs and supports both ISO images and physical CD/DVD-ROM drives.

Enhancement

None

1.1.24 FSFD-010702 USB Controller

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

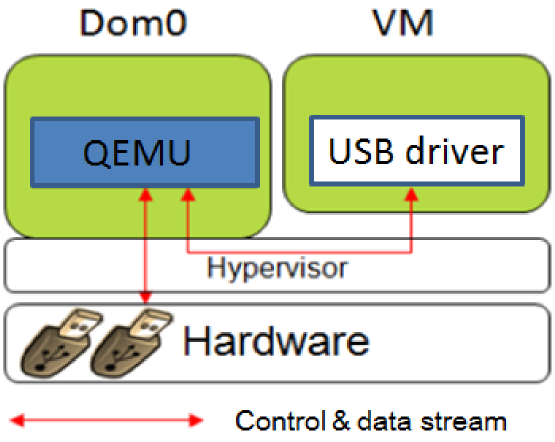
USB Controller allows VMs to use USB 2.0 devices inserted into the physical server.

Benefits

This feature helps users to reduce costs on independent USB hubs and USB over IP technologies.

Description

This feature uses Quick EMUlator (QEMU) to simulate a virtual USB device for a VM. Any requests sent from the VM to the virtual USB device are captured by the hypervisor and forwarded to QEMU. QEMU communicates with the physical USB device to process the requests, as shown in the following figure.



Enhancement

None

1.1.25 FSFD-010703 Graphics Processing Unit

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Graphics Processing Unit (GPU) allows VMs to provide 4 MB video RAM using Cirrus VGA.

Benefits

This feature allows users to view a graphical interface when they remotely access VMs.

Description

This feature provides basic graphics processing functions for VMs. If a VM runs large graphics, applications, or video games, use the GPU Passthrough feature.

Enhancement

None

1.1.26 FSFD-010705 GPU Passthrough

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

GPU Passthrough provides advance graphics processing functions for VMs, including 3D graphics processing capabilities and graphics compute acceleration capabilities.

Benefits

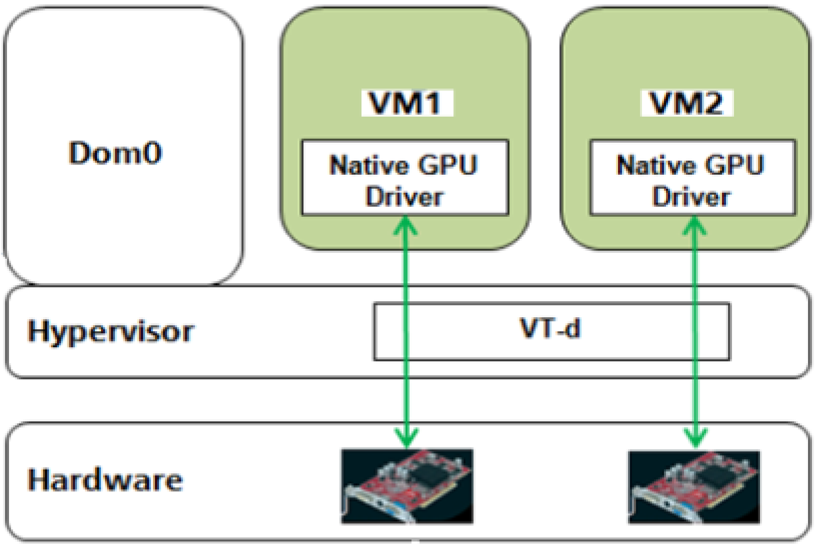
This feature accelerates graphics processing and enhances user experience on the desktop cloud. This feature allows VMs to support high-end GPU applications (such as workstation-class graphics applications and GPU-accelerated applications for high-performance computing) and provides near-native GPU performance.

Description

This feature uses VT-d/IOMMU to pass through a physical GPU to a VM.

The hypervisor handles only GPU device peripheral component interconnect (PCI) access and port I/O. Performance-consuming tasks, such as data processing, direct memory access (DMA), and Memory-mapped I/O (MMIO), are handled directly by the GPU hardware. Therefore, the VM with GPU Passthrough enabled can provide near-native GPU performance.

The following figure shows how GPU Passthrough works.



Feature Interactions

Binding a GPU to a VM has the following impacts on the VM:

- VM HA: The VM bound with a GPU does not support the HA feature.
- VM live migration: The VM bound with a GPU does not support the live migration feature.
- VM hibernation: The VM bound with a GPU cannot be hibernated.
- VM snapshot: Snapshots cannot be created for the VM bound with a GPU.
- Online VM cloning: The VM bound with a GPU cannot be cloned.
- VM export: The VM bound with a GPU cannot be exported.
- Cluster scheduling policy: The cluster scheduling policies are invalid for the VM bound with a GPU.
- VNC login: The VM for which the bound passthrough GPU has taken effect cannot be logged in to using VNC.

Enhancement

None

1.1.27 FSFD-010706 GPU Virtualization

Availability

This feature was first available in FusionSphere 5.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

GPU Virtualization is mainly used in the VDI solution for image and video editing.

Benefits

- Based on integrated computing resources, this feature provides balanced compatibility and performance for graphics processing capabilities. Data security is also enhanced for GPU capabilities. Graphics data is processed and stored on the graphics workstation, thereby minimizing the possibility of leaking enterprise graphic designs, improving information security, and reducing information management costs. Centralized IT resource management helps reduce the management cost of the IT support system.
- This feature allows end users to connect to their graphics processing desktops to process graphics from any client, anytime, and anywhere.
- This feature allows multiple VMs to share one physical GPU, thereby reducing costs.

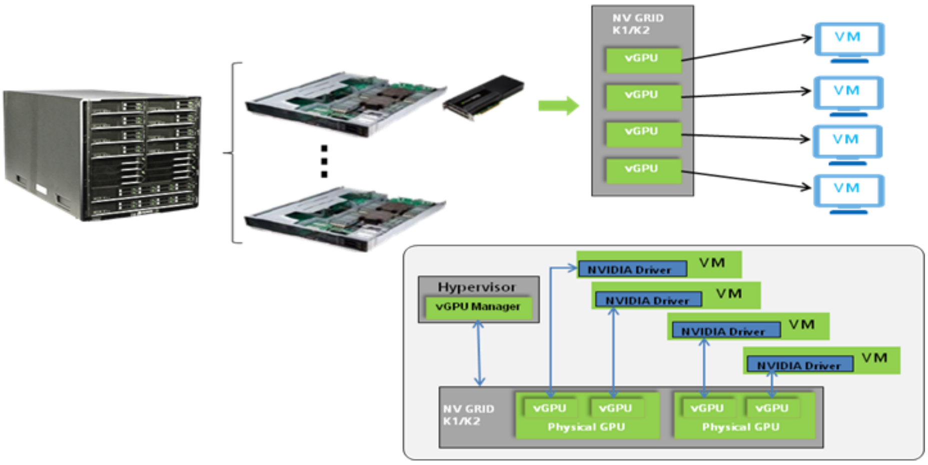
Description

With this feature enabled, a GPU client possesses the GPU acceleration capability. The image processing software uses the GPU to perform hardware rendering. Then the GPU client places the rendered bitmaps to the GPU video buffer and displays content in the buffer to the desktop access terminal in real time. VMs in the FusionSphere system support the core technology for displaying virtual desktops. Each vGPU-enabled VM sends rendering and controlling commands to the physical GPU through an independent channel. After the rendering is complete, the driver sends the desktop frames to the VMs, and then the frames are sent to the client using the remote desktop protocol.

A single server with this feature enabled supports a large number of GPU virtual desktop users and achieves a balance among GPU performance, user density, and cost performance.

One GRID K1 card can be virtualized into four pGPUs or 32 vGPUs.

One GRID K2 card can be virtualized into two pGPUs or 16 vGPUs.



Enhancement

None

1.2 Network Virtualization

1.2.1 FSFD-020101 Elastic Virtual Switch

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

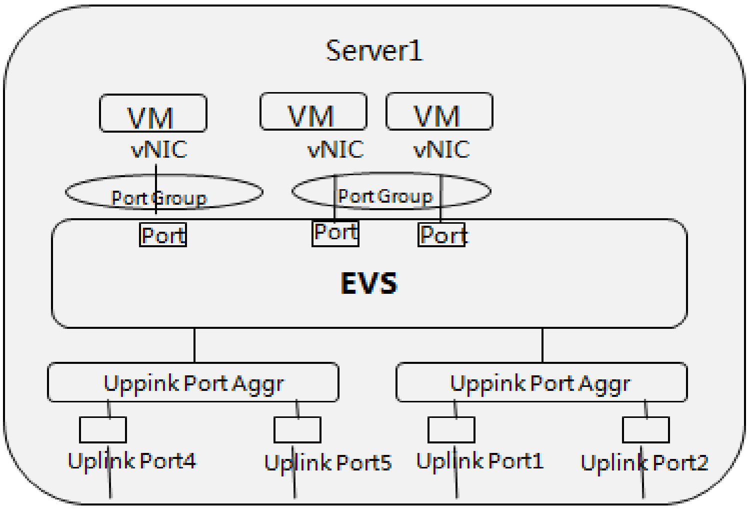
Summary

Elastic Virtual Switch (EVS) brings a new virtual switching mode to VM networks, providing virtual local area networks (VLANs) and network functions, such as DHCP quarantine, bandwidth limiting, and priority settings. All the services are highly scalable.

Benefits

This feature provides basic switching capabilities for VMs.

Description



An EVS is deployed on a host, providing switching services. The EVS connects VM NICs and host NICs to implement data transmission between the internal network and the external network. All switching data of VMs are sent through the physical NIC on the host.

- Port

  A port consists of multiple network attributes, including bandwidth QoS, layer 2 security attributes, and VLAN ID. Each EVS has multiple ports.

- Port group

  A port group consists of multiple ports with the same attributes. Administrators can configure the following attributes for a port group:

  - Bandwidth QoS

- Layer 2 security attributes

  IP-MAC addresses binding

  DHCP quarantine
- VLAN ID

Port group attribute changes do not affect VM running.

- Uplink

  An uplink connects the host and the EVS. Administrators can query information about an uplink, including its name, ratio, mode, and status.
- Uplink port aggregation

This function allows multiple physical ports on a host to be bound as one port to connect to VMs. Administrators can set the bound port to loading balancing mode or active/standby mode.

An EVS allows virtual switch ports (VSPs) on it to connect to VM NICs, so that users can query VM network traffic, implement DHCP quarantine, and configure network QoS.

Enhancement

None

1.2.2 FSFD-020102 Distributed Virtual Switch

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

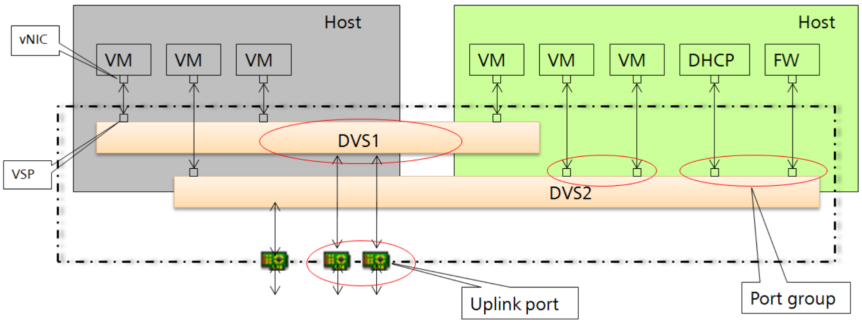
A distributed virtual switch (DVS) allows administrators to configure and maintain physical and virtual ports of virtual switches on multiple hosts.

Benefits

This feature implements centralized in management for virtual networks when a large number of hosts are deployed.

Description

The following figure shows the DVS model.



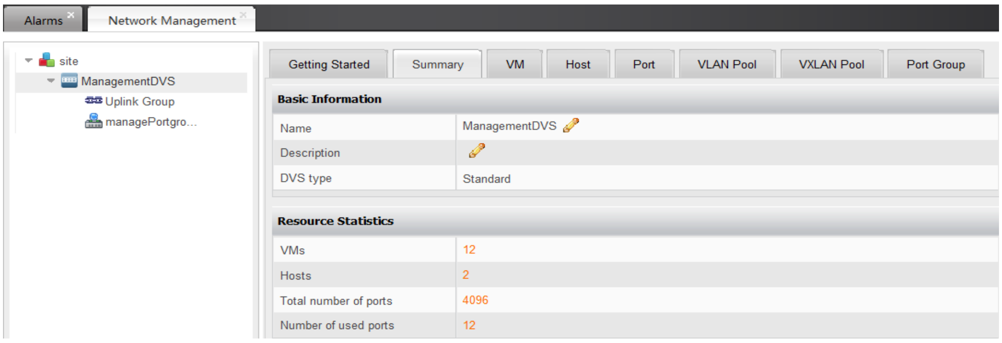
The DVS switching mode has the following characteristics:

- Multiple DVSs can be deployed in the system, and each DVS can serve multiple hosts in a cluster.
- A DVS provides several VSPs, each of which has its own attributes, such as the VLAN ID, bandwidth, priority, and DHCP quarantine setting. The ports with the same attributes are allocated to one port group for ease of management.
- Each DVS is connected to an uplink group to enable external communication for VMs. An uplink group consists of multiple physical NICs, and different load-balancing policies can be set for each physical NIC.
- Each VM provides multiple virtual network interface card (vNIC) ports, which connect to VSPs of the switch in a one-to-one mapping scheme.

This feature provides the following functions:

- Unified virtual network management

  A centralized portal is provided for ease of virtual network deployment and management. On this portal, administrators can create and manage a DVS that has multiple port groups.



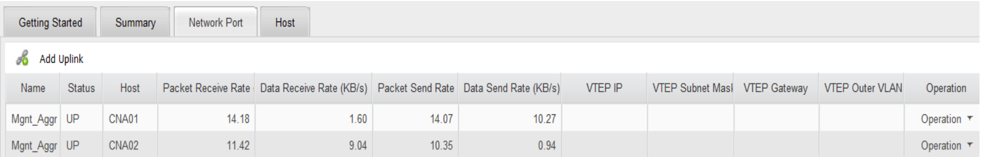
Basic Information

Name	ManagementDVS
Description	
DVS type	Standard

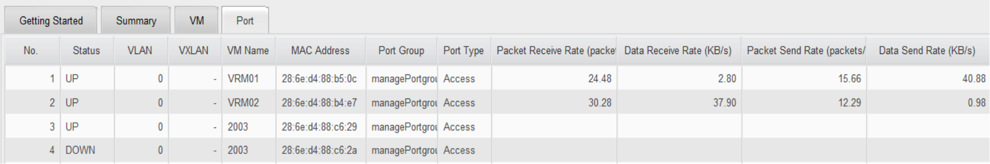
Resource Statistics

VMs	12
Hosts	2
Total number of ports	4096
Number of used ports	12

- Virtual network monitoring



Name	Status	Host	Packet Receive Rate	Data Receive Rate (KB/s)	Packet Send Rate	Data Send Rate (KB/s)	VTEP IP	VTEP Subnet Masl	VTEP Gateway	VTEP Outer VLAN	Operation
Mgnt_Aggr	UP	CNA01	14.18	1.60	14.07	10.27					Operation ▾
Mgnt_Aggr	UP	CNA02	11.42	9.04	10.35	0.94					Operation ▾



No.	Status	VLAN	VXLAN	VM Name	MAC Address	Port Group	Port Type	Packet Receive Rate (packe	Data Receive Rate (KB/s)	Packet Send Rate (packets/	Data Send Rate (KB/s)
1	UP	0	-	VRM01	28:6e:d4:88:b5:0c	managePortgrou	Access	24.48	2.80	15.66	40.88
2	UP	0	-	VRM02	28:6e:d4:88:b4:e7	managePortgrou	Access	30.28	37.90	12.29	0.98
3	UP	0	-	2003	28:6e:d4:88:c6:29	managePortgrou	Access				
4	DOWN	0	-	2003	28:6e:d4:88:c6:2a	managePortgrou	Access				

DVSs report information concerning uplinks, bound ports, and VSP traffic carried on the switch. All the statistics are displayed on the portal.

- Distributed virtual port group

  A distributed virtual port group consists of ports on a DVS. NICs connected to ports in the same port group share the same network attributes, such as bandwidth limiting, VLAN ID, subnet, DHCP quarantine setting, and IP-MAC addresses binding.

  Administrators can manage and configure port groups on the unified portal, thereby simplifying the configuration of VM port attributes.

- Distributed virtual uplink

  A distributed virtual uplink connects physical hosts and DVSs. One DVS can connect to or bind with ports on multiple hosts.

- VLAN

  VLANs comply with IEEE 802.1Q standards.

  IEEE 802.1Q VLAN tagging applies to uplinks or all inbound flows to user VMs to isolate traffic, thereby enhancing network security. This function also restricts the scope of the layer-2 broadcast domain.

- Network migration

  This function allows original network configuration data and network monitoring data to be moved to a new network during VM migration free of network interruption or need for reconfiguration.

- Layer 2 network security

  This function prevents IP or MAC address spoofing and DHCP server spoofing for user VMs.

  IP-MAC address binding prevents IP address or MAC address spoofing initiated by changing the IP address or MAC address of a VM NIC, thereby enhancing network security of user VMs.

  DHCP quarantine blocks users from unintentionally or maliciously enabling the DHCP server service for a VM, ensuring common VM IP address assignment.

Enhancement

None

1.2.3 FSFD-020103 Network QoS

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

Network Quality of Service (QoS) supports traffic shaping and bandwidth priority controls for virtual network interface cards (iNICs) and system ports.

Benefits

This feature ensures service quality of the communication between user VMs and the network plane.

Description

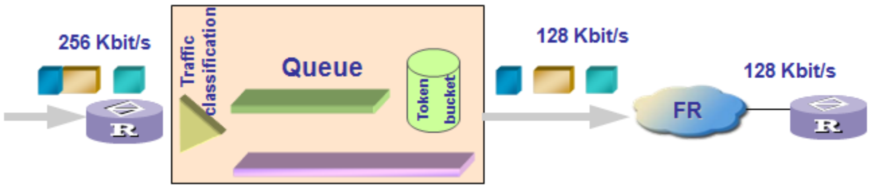
Traffic shaping optimizes network performance and reduces latency. Generally, traffic jitter may occur on a network due to the packet transmission mechanisms, such as aggregation upon interrupts, supported by different application software, network devices, and OSs used in the network. Due to the jitter, the network traffic may briefly exceed the upper limit, for example, for 0.1 μs.

Though jitter is allowed within a certain period, for example, 1 ms, if the upper bandwidth limit is set without traffic shaping enabled, the excess packets will be dropped and services will be adversely affected if the instantaneous transmission rate exceeds the predefined upper limit.

For example, if some Transmission Control Protocol (TCP) packets are dropped, the TCP sliding window will shrink, thereby slowing down packet sending and causing service unsteadiness.

Traffic shaping can reduce the possibility of packet dropping based on the configured average traffic bandwidth, peak bandwidth, and burst size. With these parameters configured, the system allows the maximum traffic bandwidth to reach the peak rate for a duration in which the average traffic bandwidth does not exceed the specified traffic burst size if sufficient network resources are available.

The following figure shows the traffic flow with traffic shaping enabled.



FusionSphere 5.1 supports the following network QoS functions:

- Outbound traffic shaping for a port group (including average send bandwidth, peak send bandwidth, and send burst size)
- Inbound traffic shaping for a port group (including average receive bandwidth, peak receive bandwidth, and receive burst size)
- Send bandwidth priority configuration for a port group
- Outbound traffic shaping for a system port (including average send bandwidth, peak send bandwidth, and send burst size)
- Send bandwidth priority configuration for a system port

Enhancement

None

1.2.4 FSFD-020104 VLAN Trunk

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite standard edition or above.

Summary

As a gateway node, a VM may require hundreds of VLANs to implement communication. However, if multiple networks are added to a VM, the VM will have too many vNICs, which are difficult to dynamically change. The VLAN Trunk feature resolves this issue. A vNIC with its **vlan_mode** set to **trunk** and with a VLAN tag configured can support the VLAN Trunk feature.

Benefits

This feature allows a single vNIC to carry packets from different VLANs, thereby enabling one VM to communicate with other VMs.

Description

A vNIC communicates with a virtual switch through virtual ports. vNIC ports can be configured as virtual trunk ports to carry traffic tagged with specified VLAN IDs.

Enhancement

None

1.2.5 FSFD-020201 SR-IOV

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite standard edition or above.

Summary

Single-root I/O virtualization (SR-IOV) allows a VM to exclusively use a NIC on the physical server to improve network traffic processing capabilities.

Benefits

This feature improves network performance and reduces latency for VMs, thereby enhancing user experience.

Description

Most commercial 10GE NICs support the SR-IOV technology. This technology allows a physical NIC to create multiple physical functions (PFs), each of which provides multiple virtual functions (VFs).

This feature allows a VM to exclusively use a VF that is derived from a PF. The VM can then directly use physical NIC resources without CPU overhead caused by virtual switching. Therefore, this feature improves network performance and reduces latency for VMs.

This feature allows VLANs and MAC addresses to be configured for virtual switching, and also provides the QoS control function based on PCIe VFs.

This feature is commercially used under some restrictions and is incompatible with the following functions:

- VM hibernation, wakeup, and live migration
- VM memory overcommitment, memory snapshot, and consistency snapshot
- VM fault tolerance
- vNIC or memory hot add or deletion

This feature has the following constraints:

- If SR-IOV is enabled, a physical NIC on a host provides virtual NICs to VMs in passthrough mode rather than providing an uplink for the virtual switches. If the physical NIC is to be used in a storage or system port, disable the SR-IOV feature.
- Intel 82599 NICs do not support maximum transmission units (MTUs) that are greater than 1500. vNIC passthrough does not support Jumbo Frame.
- This feature can be enabled only in VDI scenarios and supports only 64-bit Windows 7 OSs.
- This feature supports only Intel 82599 and Emulex BE3 NICs. The Intel 82599 NIC supports a maximum of 63 virtual functions (VFs), and the Emulex BE3 NIC supports a maximum of 28 VFs.
- SR-IOV NICs can be provided only for the service plane.
- This feature does not support the VXLAN, security group, port mirroring, and ACL functions.

Enhancement

None

1.2.6 FSFD-020302 VLAN Pool

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

VLAN Pool provides virtual local area networks (VLANs) for port groups on DVSs.

Benefits

This feature allows users to specify VLAN ID ranges.

Description

The system allocates VLANs in a VLAN pool to DVSs.

Enhancement

None

1.3 Storage Virtualization

1.3.1 FSFD-030101 Virtual Storage QoS

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Virtual Storage QoS allows users to set an input/output (I/O) upper limit for each VM volume. Any I/O operation from the backend storage device on the VM cannot exceed the specified I/O limit.

Benefits

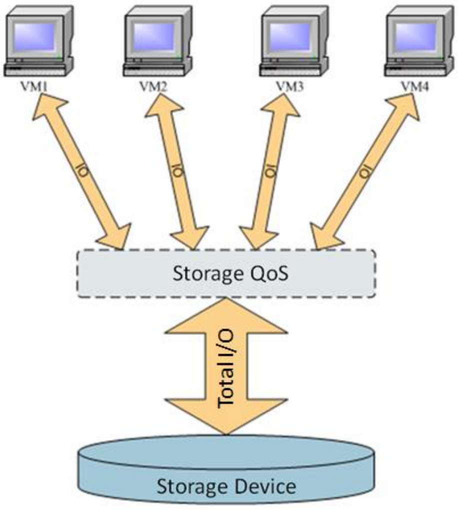
The I/O upper limit controls the ability of a VM to obtain storage resources. Therefore, among the VMs attached to the same storage device, I/O-extensive VMs or VMs with abnormal storage I/O will not affect other VMs' access to the storage device.

Description

With Storage QoS enabled, the system controls the storage input/output operations per second (IOPS) upper limit at the block I/O (BIO) layer. This layer writes the mappings between the upper limits and the corresponding device IDs in the configuration files.

After a VM sends a BIO request, the system checks whether the current amount of data to be transferred is within the configured IOPS upper limit. If not, the system blocks the BIO request, puts it into a temporary queue, and sends it at an off-peak time. Therefore, the I/O bandwidth can be controlled within the set limit.

The following figure shows the working mechanism.



Enhancement

None

1.3.2 FSFD-030102 Raw Device Mapping

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite standard edition or above.

Summary

Raw device mapping (RDM) allows VMs to directly access logical unit numbers (LUNs) on physical storage devices.

This feature allows a VM to identify Small Computer System Interface (SCSI) disks by physical device mapping information and issue SCSI commands to the host. The host then transparently transmits the commands to the storage device and returns the response message to the VM.

Benefits

This feature allows the Oracle RAC database to run on VMs.

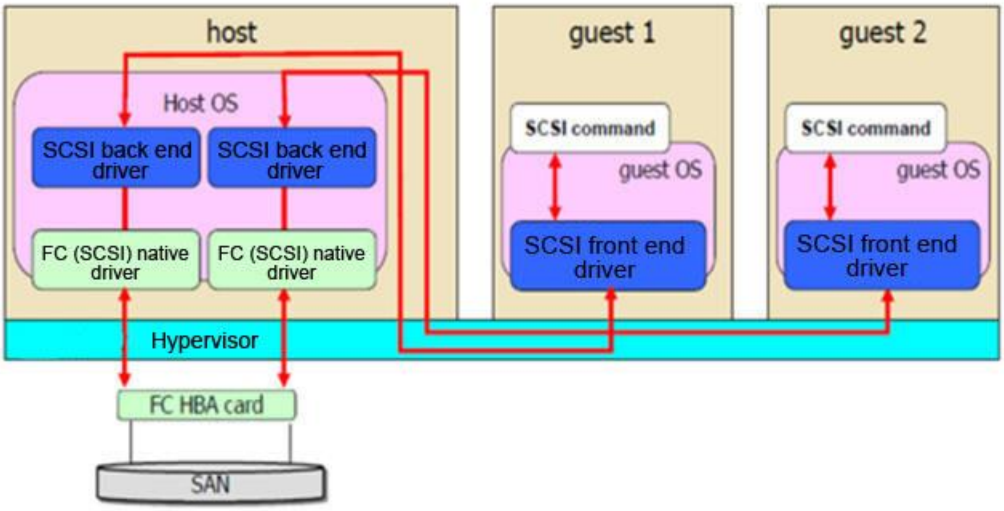
Description

This feature uses the paravirtual SCSI (PVSCSI) technology to enable VMs to directly access LUNs on a physical device.

PVSCSI functions using two types of drivers. One is a SCSI front end driver, which is installed on a VM using a paravirtualized (PV) driver. The other is a SCSI back end driver, which runs on the OS as a Linux Kernel module. Only PV drivers of Linux VMs that run the Red Hat 5.4, 5.5, 6.1, or 6.2 64-bit OS support front end drivers.

If the Oracle RAC service is deployed on a VM, the VM issues SCSI commands to the SCSI disk that is mapped to the VM. During the issuing process, the SCSI front driver sends the commands to the back end, and the back end transparently transmits the commands to the storage device and returns the response message from the physical storage device to the VM.

The following figure shows how PVSCSI works.



Enhancement

None

1.3.3 FSFD-030103 Virtual File System

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

A Virtual Image Management System (VIMS), a high-performance cluster file system, allows FusionSphere to use data stores converted into VIMS format and attaches the data stores to hosts. VIMS enables multiple VMs to gain access to an integrated storage pool to improve resource utilization. The VIMS is the basis for virtualizing multiple storage servers and provides the following services:

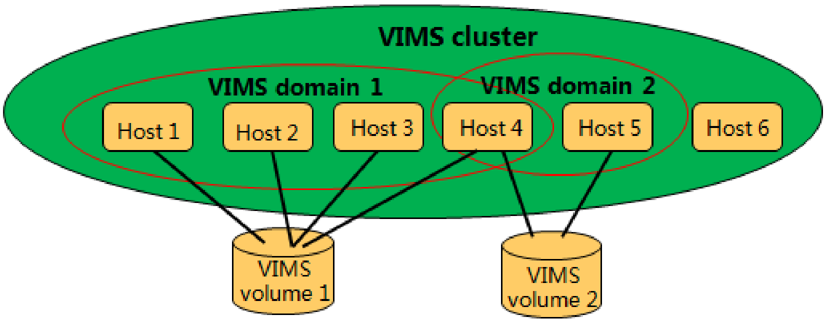
- Storage live migration
- Storage DRS
- High availability (HA)

Benefits

- This feature simplifies system management. This feature also provides convenient and reliable storage services. It allows concurrent access from multiple nodes and prevents one image file from being accessed by multiple VMs.
- This feature supports heterogeneous storage devices and various protocols, including local storage, Fibre Channel (FC) storage, and iSCSI storage. The VIMS can manage these resources in a flexible manner.

Description

VIMS enables storage resource to be used across storage systems. The following figure shows how multiple hosts with multiple VMs can use VIMS to share a clustered pool of storage.



As shown in this figure, Host 1 to Host 4 belong to the same VIMS domain and share VIMS volume 1. Host 4 and Host 5 belong to another VIMS domain and share VIMS volume 2.

Each host in a VIMS domain can connect to the VIMS volume in the domain. The VIMS provides the distributed lock management that balances access, enabling hosts to share the clustered pool of storage.

The VM files of each host are stored on the specified sub-directories in the VIMS. When a VM is running, the VIMS locks the VM files to ensure shared reading and exclusive writing on the files.

The VIMS has the following characteristics:

- Hierarchical directories
- Application to clustered VMs
- Distributed lock management and logical volume management
- Scaling among multiple storage disks and dynamic data store expansion
- Quick restoration on clustered file systems with logs
- Independent encapsulation for a VM file

Enhancement

None

1.3.4 FSFD-030104 Virtual Storage Thin Provisioning

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Thin provisioning of virtual storage resources enables flexible, on-demand allocation of storage space, which improves storage utilization.

Different from traditional thick provisioning, thin provisioning provides more storage space than the physical host has available. The system allocates physical storage space only when data is written into the virtual storage, thereby improving storage utilization.

Benefits

This feature increases storage usage and reduces the storage cost.

Description

This feature is configured for virtual disks of specified levels. Administrators can set a disk to common or thin-provisioning mode.

For a thin-provisioned disk, the system allocates part of the configured disk capacity during the first round of resource allocation, and allocates the remaining disk capacity based on the storage usage of the disk until all the configured disk capacity is allocated. For example, the physical storage device provides 100 MB storage for two VMs. VM 1 is configured with 80 MB of storage and VM 2 is configured with 90 MB of storage. The system will first allocate part of storage to each VM. If VM 1 uses the entire allocated storage, the system will allocate more storage to VM 1, if storage capacity is still available, until all 80 MB are allocated to VM 1.

This feature has the following characteristics:

- Storage independent

  This feature is independent from the VM OS type or storage device hardware. It can be configured for any storage device that runs VIMS.
- Capacity monitoring

  This feature enables alarms over data store usage. If the data usage exceeds the preset threshold, an alarm will be generated.
- Disk space reclaiming

  This feature enables disk space monitoring and reclaiming. If the allocated storage space to a user is large while the space actually used is small, the system can reclaim unused space. Only New Technology File System (NTFS) VMs support this function.

Enhancement

None

1.3.5 FSFD-030105 Virtual Storage Live Expansion

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Virtual Storage Live Expansion allows the VM disk capacity to be expanded when the VM is running.

Benefits

This feature allows users to expand disk capacity without stopping or restarting VMs.

Description

Traditionally, if the used capacity of a virtual hard disk (VHD) reaches its upper limit, the administrator needs to stop the VM and expand the disk capacity. VM services must be stopped during this process.

Virtual Storage Live Expansion allows users to expand disk capacity without stopping or restarting VMs. Therefore, disk capacity expansions do not exert adverse impact on VM services.

Enhancement

None

1.3.6 FSFD-030106 Virtual Storage Migration

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

Virtual Storage Migration enables disks on VMs to be migrated to other data stores when the VMs are running without service interruption.

Benefits

This feature allows users to migrate VM storage during service running.

Description

This feature allows administrators to migrate VM disks to other data stores on the same storage device or to different storage devices. This feature implements distributed storage resource scheduling and helps ensure service continuity during device maintenance or resource scheduling.

If VMs are stopped, VM disks can also be migrated between LUNs and virtualized storage.

Enhancement

None

1.3.7 FSFD-030107 Virtual Volume Life Cycle Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Virtual Volume Life Cycle Management allows users to perform the following operations based on service load:

- Create or delete a volume.
- Attach or detach a volume.

Benefits

This feature provides basic management functions for virtual volumes.

Description

This feature allows administrators to create or delete virtual volumes on any data stores and also attach a volume to a VM or detach the volume from a VM.

Enhancement

None

1.3.8 SFD-030201 LUN Discovery and Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

Storage Management is a basic function of storage virtualization. Storage management aggregates different physical storage resources and provides unified data stores. Storage Management also allows administrators to manage storage resources in a simple and flexible manner.

Benefits

This feature provides basic virtual storage management functions.

Description

The FusionSphere system virtualizes physical storage resources on physical storage devices. These virtualized storage resources are presented as data stores, the storage units in the virtualization system. As such, storage management is implemented based on the VM data (disks or other running status data) stored in the logical repositories (data stores, which work like file systems). Data stores can combine storage devices of different types and provide a unified model to store VM files. Data stores can also store VM templates and VM snapshots.

The FusionSphere system supports the following storage devices:

- IP SAN and FC devices based on VIMS
- Network attached storage (NAS) devices based on NFS
- Local disks on hosts

FusionSphere 6.1 supports OceanStor V3 advanced storage when FusionSphere OpenStack is deployed. In server virtualization scenarios, the V3 advanced SAN storage can be used only in the SAP HANA solution.

FusionCompute using the V3 advanced SAN storage has the following constraints:

- Each VRM can connect to multiple sets of storage devices. Each set of storage device can use only one access type (iSCSI or FC).
- Each host uses only one access type (iSCSI or FC). One datastore corresponds to one storage pool. Users can configure servers associated to the datastore and therefore determine the storage access type for each server on the VRM.
- The number of volumes must be less than or equal to the number of LUNs for the storage. In the backup scenario, the total number of volumes and snapshots must be less than or equal to the total number of LUNs and snapshots for the storage.
- V3 advanced SAN storage supports only Huawei multipathing.
- One VRM cannot connect to both LUNs and advanced SAN storage.
- If one VRM connects to advanced SAN storage, an NAS storage resource pool can connect to only the data plane of FusionCompute.
- One VRM can connect to both advanced SAN storage and FusionStorage, but volumes from either of the resource pools cannot be copied or migrated to another one.
- If one VRM connects to two sets of V3 storage (advanced SAN storage), volumes from either of the set cannot be copied or migrated to another set. Advanced SAN storage using raw device mapping (RDM) does not support hot migration.
- For each VRM, at most 15 FusionCompute ports can be configured for each set of storage.
- One VRM can connect to both advanced SAN storage and local storage (block and virtualized storage), but volumes from either of the resource pools cannot be copied or migrated to another one.
- For details about the compatibility of V3 advanced SAN storage, see *FusionSphere SIA 1.3.10.270 Compatibility List 01*. The link of obtaining this document is as follows:

  http://support.huawei.com/carrier/docview!docview?detailId=PBI1-21579393&path=PBI1-21430725/PBI1-21430806/PBI1-21431666/PBI1-21462737/PBI1-19916941/PBI1-19918232/PBI1-21579393/PBI1-22593452&nid=DOC1000400407

Enhancement

None

1.4 Interface Openness

1.4.1 FSFD-040101 Open APIs

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

Open APIs allow users to connect their own business operation systems to the cloud platform. After a user's business operation system is connected to the cloud platform, the user can provision cloud services and manage end users on their own business operation system.

Benefits

This feature allows users to provision cloud services and manage end users on their own business operation systems.

Description

The open APIs provided by FusionSphere allow users to provision services and manage end users using their own management systems. The users can add and cancel cloud services using the APIs.

These APIs are developed based on Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). Both SOAP and REST APIs are supported in IT scenarios, whereas only REST APIs are supported in ICT scenarios.

In FusionSphere 5.1, REST APIs provide the following capabilities:

- VDC, VDC quota, user, and user rights management
- Life cycle management for application instances, VMs, volumes, and software packages
- Provisioning of various services, including VPC, firewall, elastic IP address, DNAT, security group, VLAN, and VPN
- System monitoring, alarm generation, and report management

Enhancement

None

1.4.2 FSFD-040102 SNMP Interface

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

FusionManager supports Simple Network Management Protocol (SNMP) northbound interfaces for reporting alarms and monitoring information.

SNMP is an application-layer protocol that is used mostly in network management systems to monitor network-attached devices.

Benefits

This feature allows users to obtain alarms and monitoring information from FusionManager.

Description

After a device connects to FusionManager, FusionManager automatically reports alarms and monitoring information to the third-party NMS system using the SNMP interface.

The third-party NMS system can also use the SNMP interface to query alarms and monitoring information from FusionManager.

Enhancement

None

1.5 Compatibility

1.5.1 FSFD-040201 Server Compatibility

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

FusionSphere supports x86 servers from mainstream vendors.

Benefits

This feature allows customers to flexibly choose desired servers from various x86 servers to suit their business requirements.

Description

For the servers that have passed the compatibility test, use Huawei FusionCloud Compatibility Check Assistant. The link of obtaining this tool is as follows:

http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.en.jsp

Huawei FusionSphere 5.1 supports x86 servers from various vendors. The compatibility list describes the models and versions of the servers that have passed the compatibility tests.

FusionSphere 5.1 also supports the servers that meet the minimum configuration requirements for building up the FusionSphere system even they are not listed in the table. To use the supported but not listed servers in the project, the system may require adaptation and verification during project implementation.

Constraint: The CPUs of the servers must support hardware virtualization technologies VT-x and AMD-V. Otherwise, system performance will deteriorate by about 40%. The CPUs used by the servers in one cluster must be of the same vendor. Otherwise, VM migration or HA implementation may fail.

Enhancement

None

1.5.2 FSFD-040202 Storage Compatibility

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

FusionSphere supports storage devices from mainstream vendors.

Benefits

This feature allows customers to flexibly choose desired storage devices to suit their business requirements.

Description

For the storage devices that have passed the compatibility test, use Huawei FusionCloud Compatibility Check Assistant. The link of obtaining this tool is as follows:

http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.en.jsp

Huawei FusionSphere 5.1 supports IP SAN and FC SAN storage devices from various vendors. The compatibility list describes the storage devices that have passed the compatibility tests. To use the supported but not listed storage devices in the project, the system may require adaptation and verification during project implementation.

Huawei FusionSphere supports the NFS V3-enabled NAS devices.

Enhancement

None

1.5.3 FSFD-040203 Network Compatibility

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

FusionSphere supports network devices, including switches, firewalls, and load balancers, from mainstream vendors.

Benefits

This feature allows customers to flexibly choose desired network devices to suit their business requirements.

Description

For the network devices that have passed the compatibility test, use Huawei FusionCloud Compatibility Check Assistant. The link of obtaining this tool is as follows:

http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.en.jsp

Huawei FusionSphere 5.1 supports network devices from various providers. The compatibility list describes the recommended network device models.

Constraints: The elastic IP address feature (also called static public IP address) is unavailable if a third-party firewall is used. Without this feature, a public IP address, instead of being automatically assigned to a VM, can only be manually set on VMs.

The audit function of the firewall must be disabled. Otherwise, the auditing results may be distorted.

Enhancement

None

1.5.4 FSFD-040204 Operating System Compatibility

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

FusionSphere supports a variety of guest OSs from mainstream vendors to suit specific requirements of different scenarios.

Benefits

This feature allows users to flexibly choose guest OSs to suit their business requirements.

Description

For details about supported guest OSs, use Huawei FusionCloud Compatibility Check Assistant. The link of obtaining this tool is as follows:

http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.en.jsp

Enhancement

None

1.5.5 FSFD-040205 Browser Compatibility

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

FusionSphere supports mainstream browsers, including Internet Explorer, Mozilla Firefox, and Google Chrome.

Benefits

This feature allows users to flexibly choose browsers to log in to the FusionManager portal for cloud platform management.

Description

Browsers supported by FusionSphere include:

- Internet Explorer 9, 10, or 11
- Mozilla Firefox 21 or later
- Google Chrome 21 or later

Enhancement

None

1.6 Active-Standby DR

1.6.1 FSFD-050101 Storage Replication-based DR

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization platinum edition or operation edition. The feature can also be sold independently.

Summary

Storage Replication-based Disaster Recovery (DR) allows two sites far from each other to use a Huawei storage device (with its synchronous or asynchronous replication function) and the Ultra Virtual Replication (UltraVR) DR management software to implement DR.

Benefits

This feature shortens the service downtime and reduces losses incurred by disasters.

Description

Storage Replication-based DR enables the system to use the remote replication function of the Huawei storage device to remotely replicate the VM disk data stored at the production site to the DR site.

The UltraVR software is used to replicate the VM configuration data, such as the VM CPU, memory, NIC, and disk attributes, from the production site to the DR site and to manage the system DR plan. If a disaster occurs at the production site and causes VM failures, administrators can start the DR plan to restore the VMs using the VM configuration data and disk data backed up at the DR site. In this manner, the DR site can take over services from the production site and ensure service continuity.

The Storage Replication-based DR plan applies to the following DR scenarios:

- Active-standby DR

  In this scenario, a production site and a DR site are set up. Normally, only the production site provides services. If a disaster occurs at the production site, services are automatically switched over to the DR site.
- Active-active DR

  In this scenario, two duplicate sites are set up. Both sites function as production sites to provide services, and either site also functions as the DR site of the other one. If a disaster occurs at one site, services are automatically switched over to the other site.
- Shared DR

  In this scenario, multiple production sites and a shared DR site are set up. Normally, all production sites provide services at the same time, and the DR site is on standby. If a disaster occurs at any of the production sites, services are automatically switched over to the shared DR site.

The Storage Replication-based DR feature enables the system to provide the following functions:

- Centralized recovery plan management
  - Creates and manages recovery plans.
  - Automatically discovers and displays the VMs that are protected by storage arrays.
  - Configures storage protection policies. The system synchronizes data for the protected VMs based on the protection policies used to meet recovery point objective (RPO) requirements.
  - Maps VMs to the attached resources, such as clusters and networks, at the DR site.
  - Sets VM startup priorities to meet recovery time objective (RTO) requirements of different VMs.
  - Customizes VM IP addresses.
  - Customizes low-priority VMs to stop at the DR site.
  - Sets the startup of host OS upon the host power-on at the DR site.
  - Uses the customized script to extend the recovery plan.
  - Controls access to the recovery plan based on the role-based access control function.
  - Displays the end-to-end VM protection topology.

  - Allows active-active DR or active-standby DR for two sites, or restores multiple sites as a shared DR site.
- Automatic switchover
  - Supports one-click start of the recovery plan to implement automatic service switchover from the production site to the DR site. Automatic switchover can also prevent errors caused by manual operations.
  - Automatically changes the standby LUN to the active state during the switchover.
  - Stops low-priority VMs at the DR site.
  - Automatically starts protected VMs based on the configured sequence.
  - Executes the user-defined script during the recovery.
  - Automatically reconfigures VM IP addresses at the DR site.
  - Manages and monitors recovery plan implementation.
  - Automatically monitors site availability and reports an alarm when a site is faulty.
- DR test (DR drilling)
  - Supports the one-click DR plan test to check whether the recovery plan meets the RPO and RTO requirements.
  - Supports the use of storage snapshots to test a DR plan, which has no adverse impact on the storage replication function and does not cause data loss.
  - Supports VM restoration on an isolated network, preventing adverse impacts on the application programs at the production site.
  - Customizes the restoration plan execution specific for the test plan.
  - Automatically resets the system back to the state before the test.
  - Allows test results and failover execution results to be stored, viewed, and exported.
- Planned migration
  - Supports planned migration based on the recovery plan so that VMs can be smoothly migrated from the production site to the DR site in the event of a scheduled interruption, such as a planned power outage, maintenance before an upgrade, or a foreseeable disaster.
  - Automatically stops the protected VMs at the production site before VM migration to ensure VM status consistency and to replicate all VM data to the DR site without data loss.
- Automatic DR reprotection
  - Supports one-click data replication to the production site to reprotect VMs.
  - Reversely executes the original recovery plan to switch services back to the production site.

To implement Storage Replication-based DR, ensure that the following requirements are met:

- The Storage Replication-based DR plan applies only to the server consolidation and data center virtualization scenarios.
- VMs that require the Storage Replication-based DR function must be created on the FusionManager or FusionCompute portal. Application instances created on the FusionManager portal do not support this function.
- Huawei SAN storage devices must be used as the storage devices for remote replication, and the VMs must use a Virtual Image Management System (VIMS)-based storage resource.
- When synchronous replication is used, the RPO is 0, sites are connected using optical fibers, and the distance between two sites is less than 100 km. When asynchronous replication is used, the RPO is greater than or equal to 15 minutes, sites communicate over the IP protocol, and the distance between two sites is not limited.

Enhancement

None

1.6.2 FSFD-050201 Metropolitan Active-Active DR

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization platinum edition or operation edition. The feature can also be sold independently.

Summary

Metropolitan Active-Active DR allows two sites far from each other to use the mirroring function provided by Huawei Storage and the FusionCompute high availability (HA) and dynamic resource scheduler (DRS) functions to implement DR.

Both sites can function as production sites to provide services, and each of them also serves as the DR site for each other to implement automatic switchover in the event of a disaster.

Benefits

This feature ensures zero data loss and zero RPO in the event of a disaster.

The feature also supports automatic service recovery to reduce service downtime and minimize losses incurred by the disaster.

Description

Metropolitan Active-Active DR allows two sites within 100 km to simultaneously provide services, which improves system service capabilities and resource utilization.

The two sites share resources. If one site is faulty, services are automatically switched over to the other site without data loss, and the services taken over by the DR site can recover in a few minutes.

In addition, hosts in the same cluster on the FusionCompute platform are also deployed in active-active mode at the local and remote sites. The FusionCompute VM HA function enables the system to implement automatic switchover between the two sites in the event of a disaster, and the FusionCompute DRS function allows the system to switch over host services preferentially between the local site if only some VMs are faulty.

Metropolitan Active-Active DR has the following characteristics:

- Zero data loss

  Real-time data synchronization is implemented for mirrored volumes at two sites, thereby ensuring zero RPO and I/O data consistency.

- Zero service downtime for planned migration and minute-level service downtime for service faults

  The large layer 2 networking between the two sites ensures zero RTO during planned maintenance by live VM migration. The HA function of the virtualization platform ensures the RTO is reached within minutes in the event of any service fault.

- Automatic switchover

  If a VM at one site is faulty, VM HA is triggered and services on the faulty VM are automatically switched over to a VM at the DR site. The whole process requires no human intervention, and users are unaware of the process. If the DRS function is enabled, the system implements service switchover preferentially among VMs at the local site, rather than immediately triggering switchover between the local and remote sites.

- Flexible service access

  Network, service, and storage layers of the two sites provide services in active-active mode, allowing flexible and efficient service access.

Metropolitan Active-Active DR is applicable to scenarios that have high RPO and RTO requirements, including the following:

- Service load needs to be balanced across data centers, and resource scheduling must not interrupt services.
- Services must be recovered as soon as possible if some or all services (network, storage, and host services) at a site are faulty.
- The cables connecting two data centers meet high bandwidth and low latency requirements. Usually, L1 cables are used to connect two data centers, the distance between the two data centers is less than 100 km, and the loop latency is within 1 ms.

This feature does not apply to the following scenarios:

- The distance between the production site and the DR site is greater than 100 km.
- The DR process involves a large number of VMs and requires human intervention.
- RTO tests are required.

Enhancement

None

1.7 VM Backup

1.7.1 FSFD-050301 VM Disk Backup

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

VM Backup uses Huawei eBackup software, the FusionCompute snapshot function, and the Changed Block Tracking (CBT) function to back up VM data. The eBackup software works with FusionCompute to back up the data of a VM or a specified volume of a VM to an external SAN or NAS storage device based on the specified backup policy. If a VM becomes faulty or its data is lost, the VM can be restored using its data backups.

Only support LAN-base backup. Not support LAN-free and file level backup.

Benefits

This feature allows important VM data to be rapidly restored and minimizes data loss.

Description

The VM Backup feature has the following characteristics:

- No backup agent needs to be installed on the VM to be backed up.
- VM data can be backed up regardless of whether the VM is in the running or stopped state.
- Backup and restoration can be performed for VMs using different storage resources, such as FusionStorage or virtualized storage resources.
- VM data can be backed up to various storage devices, including external SAN or NAS storage devices.
- Application-consistent backup and recovery are provided by leveraging Microsoft's Windows Volume Shadow Copy Service (VSS). VSS provides a consistent interface that allows coordination between user applications that update data on disk and those that back up applications.
- Multiple backup modes, including full backup, incremental backup, and batch backup are supported.
  - Full backup allows the system to back up only valid data.
  - Incremental backup allows the system to back up only the data blocks that have changed since the previous backup. Therefore, less data needs to be backed up, reducing VM backup costs and minimizing the backup window.
- Data backups can be used to restore a new VM (the whole VM), the original VM (only VM disks), or a specified VM (only VM disks) one by one or in batches. To restore a new VM (the whole VM) using the data backup, the new VM must be created on FusionCompute. Otherwise, the restoration will fail. The VM created on FusionManager or on the desktop cloud cannot be restored using the data backup.

- Multiple VM restoration modes are supported, including VM image-based restoration, incremental data-based restoration, and fine-grained file-level OS restoration.
  - When a VM image is used to restore a VM, the data to be restored is all data in a full backup.
  - Incremental VM data can only be used to restore VMs that use virtualized storage resources. When the incremental data is used to restore the original VM, the CBT function is used and only data blocks changed since the last backup need to be restored, thereby implementing quick restoration.
  - Fine-grained file-level restoration restores only some files or directories in a disk, instead of restoring the entire disk. Therefore, the fine-grained file-level restoration is the fastest and most effective restoration modes.
- When virtualized storage is used at the production site, multiple backup data transmission modes are supported, including LAN, LAN SSL, and SAN (or LAN-free). The LAN SSL encryption transmission mode secures the backup data, and the SAN (or LAN-free) transmission mode improves backup and restoration performance and reduces performance penalty on production servers. If FusionStorage is used at the production site, the internal storage network is used for backup. Therefore, the backup data has no security risks.
- eBackup supports flexible backup policies.
  - Allows users to configure differentiated backup policies for VMs or VM groups.
  - Allows users to select the VMs to be backed up by selecting a container, such as a cluster, in the hypervisor, and then automatically discovers new VMs in the selected container during the data backup.
  - Supports multiple backup modes, including full backup and incremental backup.
  - Supports deduplication and compression of backup data.
  - Allows users to configure the data backup retention duration and automatic deletion of expired data.
  - Allows users to set backup policy priorities.
- eBackup supports concurrent backup and restoration. One backup agent supports up to 40 concurrent tasks.
- VM disks can be backed up and restored across FusionCompute sites.
- The eBackup backup plan employs the distributed architecture that blends backup servers and backup agents. One backup server manages up to 64 backup agents. The backup servers can also function as backup agents. Therefore, no additional backup agent servers are required. Both backup servers and the backup agents can be centrally managed using a browser. It is recommended that each backup agent backs up data for 200 VMs. You can add backup agents based on the VM scale. A maximum of 10,000 backup agents are supported.
- The eBackup backup plan delivers high reliability.
  - If a backup agent fails, its services are distributed to other backup agents.
  - The eBackup backup system supports self-recovery in the disaster scenarios, for example, the OS, host, or storage is damaged.
- The eBackup backup plan supports easy management and maintenance.
  - The backup system can be deployed on VMs using templates or on physical servers, simplifying backup software installation and shortening the deployment time.
  - The eBackup backup system supports centralized backup, restoration, and system management using the GUI or command-line interface (CLI), which is easy and straightforward for users to perform operations.

The VM backup plan applies to the following scenarios:

- Server consolidation, data center virtualization, converged appliance, and desktop cloud.
- Storage resources at the production site are provided by FusionStorage or virtualized SAN devices, NAS devices, or local disks.

Enhancement

FusionSphere 3.1:

FusionSphere 3.1 enhances the CBT backup function. It implements differential bitmap backup and allows the CBT function to interact properly with the VM live migration, VM HA, storage migration, and offline disk capacity expansion services. It also decreases full backups caused by the CBT failure, lowers bandwidth consumption, minimizes the backup window, and reduces adverse impacts on VM performance.

FusionSphere 5.1:

FusionSphere 5.1 supports the SAN or LAN-Free transmission mode. In this mode, backup servers obtain data backups directly from the shared production FC SAN or IP SAN storage, bypassing the management or service network or production hosts. Therefore, VM restoration using backups does not consume host resources or deteriorate host performance. This feature is valid only for virtual storage.

FusionSphere 5.1 supports file-level restoration. If a VM file is damaged or deleted by mistake, this file can be restored rapidly and efficiently without the need to map the entire disk. This feature is supported by both virtualized storage and FusionStorage and is available in both server consolidation and converged appliance scenarios.

1.8 Reliability

1.8.1 FSFD-060101 Active and Standby Management Nodes Architecture

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

FusionSphere management nodes can be deployed in active/standby mode on both physical servers and VMs.

Benefits

This feature improves management system reliability.

Description

The FusionSphere management system works in active/standby mode. The active node provides services through the floating IP address.

If the active node process is faulty or the OS on the active node or the host breaks down, the standby node takes over service processing.

During the switchover, the floating IP address is configured and the MAC address is updated on the gateway. All processes monitored by the original active node start on the standby node and provide services.

The active and standby management nodes use the heartbeat detection mechanism. The standby node detects the health status of the active node in real time. Once a fault is detected, the standby management node takes over services from the active node.

FusionSphere uses databases working in active/standby mode. The active database performs data read and write operations.

If data in the active database is changed, the change will be synchronized to the standby database.

To ensure the performance of the active database, asynchronous synchronization is performed between the active and standby databases. This prevents data loss if an active/standby database switchover occurs.

Enhancement

None

1.8.2 FSFD-060102 Black Box

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Virtualization software and virtualization management software support black boxes. A black box records and stores the last records of the system to a local directory for fault locating purposes if the following faults occur on the management or computing nodes:

- System breakdown
- Process deadlock
- Unexpected server restart

Benefits

This feature allows system information before an exception to be recorded to help maintenance personnel locate and rectify system faults, improving product maintainability.

Description

The black box collects and stores diagnosis information provided by the diagnosis tool and kernel logs on the management and computing nodes before the node OS exits due to an unexpected error.

Maintenance personnel can export the information collected by the black box for analysis after the system breaks down. To ensure data security, the black box allows the collected information to be stored in a local directory.

Enhancement

None

1.8.3 FSFD-060103 Management Data Backup

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

Management Data Backup allows administrators to manually back up management data of each service in the system before performing an important operation, such as critical data modification.

The data backup can be used to restore the management data if a service becomes faulty or the operation has not achieved the expected result. This restoration can minimize impacts on services.

The management data of each service can be automatically or manually backed up.

Benefits

This feature allows prompt data restoration and minimizes adverse impacts on services.

Description

The automatic backup function is enabled by default. The management data of each service can be automatically or manually backed up.

If a third-party backup server is configured, the system automatically uploads the data that is automatically or manually backed up on the local node to the third-party backup server. All backup packages are automatically saved on the local server regardless of whether a third-party backup server is configured. The third-party backup server can be a File Transfer Protocol (FTP) server or File Transfer Protocol over SSL (FTPS) server.

If the number of backup files stored on the third-party backup server is less than the allowed maximum number, new backup files will not overwrite the existing backup files. If the number of stored backup files exceeds the maximum number, the system automatically deletes the earliest backup files. The default maximum number is 30.

Enhancement

None

1.9 VM HA

1.9.1 FSFD-060201 HA Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the cloud suite standard edition, virtualization suite standard edition, or above.

Summary

FusionSphere supports VM HA to enable faulty VMs to be automatically restarted in a specific resource pool in the event of a failure, thereby improving VM availability.

Benefits

This feature offers the following benefits:

- Relieves engineers of the need to manually restart VMs.
- Enhances VM reliability and availability.
- Shortens the service downtime.

Description

After VM HA is enabled for a cluster, administrators can enable HA for a VM during VM creation.

The FusionSphere system periodically detects VM statuses. If FusionSphere detects that a VM is faulty due to a physical server or software failure, VM HA allows the VM to be automatically restarted on another production physical server with spare capacity.

During the restart, the VM reloads the OS. Data that is not saved to the hard disk before the VM HA is lost.

If this function is not enabled for a VM, the VM stops working after a fault occurs. In this case, administrators need to manually restart the VM.

Enhancement

None

1.10 Security

1.10.1 FSFD-070101 Virtualization Antivirus

Availability

This feature was first available in FusionSphere 5.0 and requires a license of the cloud suite standard edition, virtualization suite advanced edition, or above.

Summary

Virtualization Antivirus allows the antivirus function to be implemented by a dedicated reinforced secure VM, thereby preventing the antivirus function from consuming resources on other VMs and enhancing the antivirus performance.

Benefits

This feature provides the following benefits:

- Avoids antivirus storms and improves VM user experience by 10% compared with traditional antivirus products.
- Implements central management of antivirus services. Users do not need to install and update antivirus databases on each VM.

Description

The antivirus function protects VMs against viruses. However, traditional antivirus software can protect only the VM where the antivirus software is installed. To protect all VMs on a host, users need to deploy the antivirus software on each VM, which not only consumes too many VM resources but also may cause antivirus storms during full-disk scans or virus updates. To address this issue, Huawei FusionSphere provides APIs for antivirus product vendors to develop antivirus solutions that allow antivirus software deployment on a dedicated secure VM. Then, with only a lightweight antivirus driver installed on the other VMs on the host carrying the secure VM, the system can scan and remove viruses on these common user VMs using the antivirus capabilities of the secure VM, consuming only a few VM resources.

Enhancement

None

1.10.2 FSFD-070202 Anti-IP/MAC Address Spoofing

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite standard edition or above.

Summary

FusionSphere supports IP-MAC address binding for VM NICs to prevent IP/MAC address spoofing initiated by a VM user by changing their VM IP or MAC address.

Only support static ip bind with mac.

Benefits

This feature prevents IP/MAC address spoofing initiated by a VM user and enhances virtual network security.

Description

After IP-MAC address binding is enabled for a VM, the FusionSphere system obtains and saves the mapping of the virtual port, VM IP address, and MAC address.

When a VM sends data packets, FusionSphere checks the IP and MAC addresses in the packets and permits the packets if it detects that the IP and MAC addresses are consistent with those in the mapping. Otherwise, FusionSphere discards the data packets.

To enable IP-MAC binding, the VM IP and MAC addresses must be legitimate. FusionSphere only checks Address Resolution Protocol (ARP) and IP data packets sent by VMs.

Enhancement

None

1.10.3 FSFD-070203 Rights Separation Mode

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite standard edition or above.

Summary

The FusionSphere system has three user roles: system administrator, security administrator, and security auditor. Each of these roles is granted separate and independent rights for checks and balances.

Benefits

This feature improves system security and enables FusionSphere to meet the security requirements of the defense industry.

Description

FusionSphere supports rights separation mode and provides three user roles to implement checks and balances. Checks and balances allow for a rights-based management that enables one role to limit another.

Details about the roles are as follows:

- System administrator: has all service-related rights and rights to create and delete accounts. (A system administrator cannot grant rights to accounts or manage roles.)
- Security administrator: can grant rights to accounts and manage roles and password policies.
- Security auditor: has rights to manage logs.

Enhancement

None

1.10.4 FSFD-070301 Residual Data Deletion

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

FusionSphere supports residual data deletion for VMs and VM disks.

Benefits

This feature prevents user data leaks.

Description

Residual Data Deletion overwrites all data on VM disks to ensure that the deleted data is not recoverable.

This feature provides high security, but the deletion process takes a longer time and consumes more system resources.

Enhancement

None

1.10.5 FSFD-070401 DHCP Snooping

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

DHCP Snooping is a security feature that builds and maintains a DHCP snooping binding table to filter DHCP messages received from untrusted sources.

The DHCP snooping binding table contains the MAC address, leased IP address, lease time, VLAN ID, and interface information about untrusted zones.

Benefits

This feature improves service security and prevents attacks from invalid DHCP servers.

Description

After DHCP snooping is enabled, the virtual switch monitors DHCP packets and extracts and records the IP address and the MAC address in the received DHCP Request or DHCP ACK packets. The binding between the IP and MAC addresses is remembered by the system and used for subsequent checks. Packets from incorrect IP addresses will be detected and discarded.

In addition, DHCP snooping allows a physical port to be configured as a trusted or untrusted port. The switch receives and forwards DHCP Offer packets that are sent to trusted ports and discards DHCP Offer packets that are sent to untrusted ports.

Therefore, DHCP snooping allows a switch to filter messages from invalid DHCP servers and ensures that clients obtain IP addresses from valid DHCP servers.

Enhancement

None

1.10.6 FSFD-070402 ARP Broadcast Suppression

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite standard edition or above.

Summary

FusionSphere supports ARP broadcast suppression and IP broadcast suppression for VMs.

Benefits

This feature improves service security, lowers adverse impacts on network communication caused by broadcast storms, and defends against broadcast attacks.

Description

In an elastic host leasing scenario of data center virtualization, a malicious user can lease a host and initiate broadcast attacks on other hosts, interrupting network communication. With broadcast suppression enabled on virtual switches, FusionSphere provides the broadcast suppression function to prevent broadcast attacks initiated by malicious users.

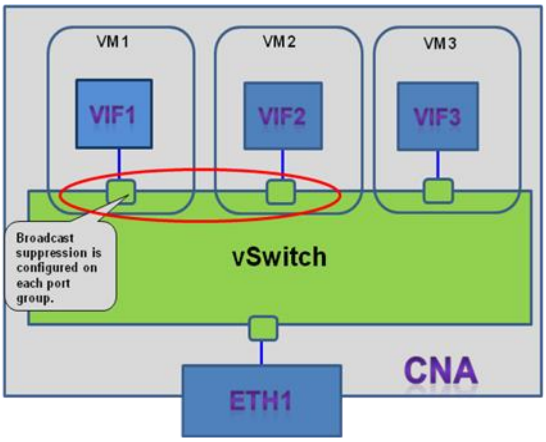
In server consolidation and desktop cloud scenarios, the probability of internal attacks is low. Therefore, broadcast suppression is disabled for virtual switches by default to avoid network performance deterioration. If the network is large or susceptible to attacks, an administrator can enable broadcast suppression.

Firewalls can be used to prevent broadcast attacks from external networks. FusionSphere also provides broadcast suppression for VM NIC outbound traffic to prevent broadcast attacks from internal networks.

On the FusionCompute portal, an administrator can enable ARP and IP broadcast suppression on a port group basis.

This feature does not support unicast packet suppression.

The following figure shows how the broadcast suppression feature is enabled on port groups.



Enhancement

None

1.11 Virtual Data Center Services

1.11.1 VM

FSFD-080101 VM Life Cycle Management

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

VM Life Cycle Management allows users to create and manage VMs on FusionManager or on an integrated service system using interfaces provided by FusionManager.

Benefits

This feature allows users to create and manage VMs based on their service demands.

Description

FusionManager allows users to create VMs in multiple modes.

- When a VM is created using the default mode, FusionManager automatically chooses a cluster and a physical server for the VM based on the resource usage and allocates required resources to the VM.
- Users can manually specify the cluster to which the VM belongs and the physical server on which the VM is running.
- Users can perform basic VM life cycle management, including creating, deleting, starting, stopping, restarting, hibernating, waking up, making a snapshot of, and restoring a VM.

Enhancement

None

FSFD-080102 Remote Connection

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

Remote Connection allows users to log in to a VM using VNC.

Benefits

This feature provides a secure and convenient channel for logging in to VMs to perform service maintenance and troubleshooting.

Description

FusionSphere supports Remote Connection to allow users to log in to a VM for service maintenance and troubleshooting.

When a user cannot log in to a VM from an external network, system maintenance personnel can log in to the VM using VNC to troubleshoot it.

Enhancement

None

FSFD-080103 VM Repair

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

VM Repair allows a VM to be restored if the VM OS fails to work properly.

VM Repair does not adversely affect the data on user data disks.

Benefits

This feature allows a VM to be restored even if the VM OS is faulty and does not cause user data loss.

Description

This feature enables FusionSphere to restore a VM by performing the following steps:

- Create a VM that has the same specifications with the faulty VM.
- Attach the system and data disks of the faulty VM to the created VM as data disks.

Enhancement

None

1.11.2 Virtual Volume

1.11.2.1 FSFD-080401 Virtual Volume Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

FusionSphere provides Virtual Volume Management for VMs to enable users to create, attach, detach, query, and delete virtual volumes.

Benefits

This feature allows users to manage virtual volumes and perform operations on them.

Description

Operations involved in Virtual Volume Management include:

- Create a virtual volume: Users can create a virtual volume by setting **BSMediaType** and **ReduceMode**. The value of **BSMediaType** can be **SAN-SSD**, **SAN-SAS&FC**, **SAN-SATA**, or **SAN-Any**. The value of **ReduceMode** can be **Yes** or **No**.
- Attach a virtual volume: Users can attach a created virtual volume to a VM.
- Detach a virtual volume: Users can detach a virtual volume from a VM to reduce the storage capacity of the VM.
- Query a virtual volume: Users can query virtual volume attributes.
- Delete a virtual volume: Users can delete a detached virtual volume so that the virtual volume cannot be used by other VMs.

Enhancement

None

FSFD-080402 Virtual Volume QoS

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

Virtual Volume QoS enables FusionSphere to support different storage media.

Benefits

This feature allows administrators to flexibly select storage media to use as the system and data volumes of VMs.

Description

This feature allows administrators to select required storage media during virtual volume creation. The storage media can be SATA and SAS hard disks or Fibre Channel (FC) storage devices.

Enhancement

None

1.11.3 Cloud Monitoring

FSFD-080501 Cloud Monitoring

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

Cloud Monitoring helps administrators learn the hardware and software operating status and identify hidden problems in a timely manner.

Benefits

This feature allows customers to perform routine maintenance based on the monitored information, improving maintenance efficiency and reducing costs.

Description

Cloud Monitoring includes topology management, monitoring management, alarm management, task center, and operation log management.

Topology Management

FusionManager provides a topology displaying all resources in the system. The topology has three views: physical resource view, cluster view, and application view.

The topology displays logical view of computing resources, storage resources, network resources, and virtual resources. It helps administrators learn the following information:

- Hardware resources: servers, storage devices, and network devices used in the system
- Application deployment: VMs on which system components, for example, the database server, are deployed, and hosts on which VMs are deployed
- VM information: attributes and states of VMs

The topology also displays node alarm status in different images based on the alarm severity.

Monitoring Management

FusionSphere monitors the usage and status of cloud resources (including computing, storage, and network resources) and displays hardware and software resources in dashboards. Administrators can export historical monitoring data.

Cluster monitoring information includes:

- Alarm statistics
- Operating status of VMs in the cluster
- Comparison of average CPU usage trend
- Comparison of average memory usage trend
- Comparison of average outbound network traffic trend
- Comparison of average inbound network traffic trend

Server monitoring information includes:

- Alarm statistics
- Operating status of the VMs on this server
- CPU usage
- Memory usage
- Inbound and outbound network traffic rates
- Disk I/O and disk usage

Storage device monitoring information includes:

- Alarm statistics
- Mounting status
- Total size
- Allocated size and available size

Network switch monitoring information includes:

- Inbound and outbound network traffic rates
- Port status
- Port data traffic

VM monitoring information includes:

- Alarm statistics
- VM status
- CPU usage
- Memory usage
- Inbound and outbound network traffic rates
- Disk I/O and disk usage

Alarm Management

FusionSphere provides a unified UI for monitoring the alarms reported by servers, switches, storage devices, and hypervisors.

FusionSphere monitors all hardware and software alarms on a cloud network, including alarms from computing devices, storage devices, and virtual resource applications.

All the alarms are displayed in a list. Administrators can view the alarms of a node in the topology view. FusionSphere also provides customized templates to facilitate alarm query.

A mail server can be configured to send email notifications for alarms generated.

By adding a third-party component, administrators can manage alarms from third-party components in SNMP trap mode on FusionManager.

FusionManager supports alarm query by the specified time range, alarm severity, alarm object, alarm ID, alarm name, and component name.

Administrators can set alarm thresholds for the CPU usage, memory usage, disk I/O, and network traffic.

The system supports the following alarm severities:

- Critical: indicates a fault that will severely affect services provided by the system if it is not rectified. This type of alarm must be handled immediately even if the fault occurs in non-working time.
- Major: indicates a fault that will affect service quality if it is not rectified. This type of alarm must be handled in a timely manner.
- Minor: indicates a fault that does not affect service quality. To prevent more serious faults, this type of alarm needs to be observed or handled if necessary.
- Warning: indicates a fault that may affect service quality. This type of alarm must be handled based on the error type.

Enhancement

None

1.11.4 Network QoS

FSFD-080601 Network QoS

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

Network QoS allows administrators to set the inbound and outbound network traffic rates and data packet forwarding priorities.

Benefits

This feature allows users to set a network transmission capacity to meet the network transmission requirements of different services.

This feature also ensures that network transmission capacities are not affected by service changes.

Description

FusionSphere allows administrators to set the average send and receive bandwidth and the burst size for inbound and outbound traffic to facilitate traffic management of applications on the network.

Enhancement

FusionSphere 3.1 added management of burst send traffic and receive traffic.

1.11.5 Virtual Private Cloud Services

FSFD-080801 VPC Management

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

A virtual private cloud (VPC) provides an exclusive, isolated network container for application instance provisioning.

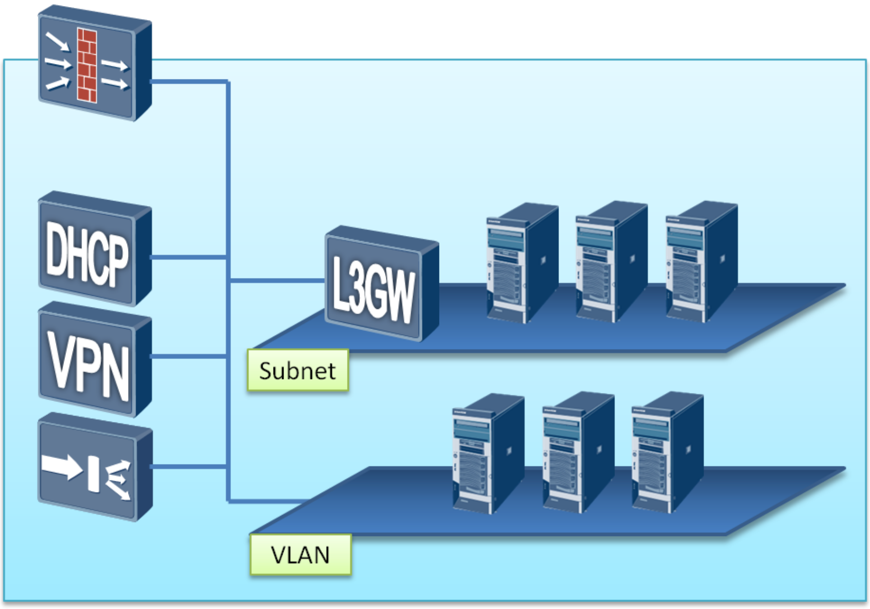
Benefits

This feature isolates application instances and network resources.

Description

In virtual data center solutions, different departments or services can be isolated using VPCs. A VPC functions as a secure network that provides the following elements:

- A virtual firewall
- Multiple network planes



Enhancement

None

1.11.5.1 FSFD-080803 VPC Network Management

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

VPC Network Management allows users to manage VPC networks that consist of internal networks.(Not support direct networks and routed networks)

Benefits

This feature enables users to select direct networks, routed networks, and internal networks for communication based on application requirements.

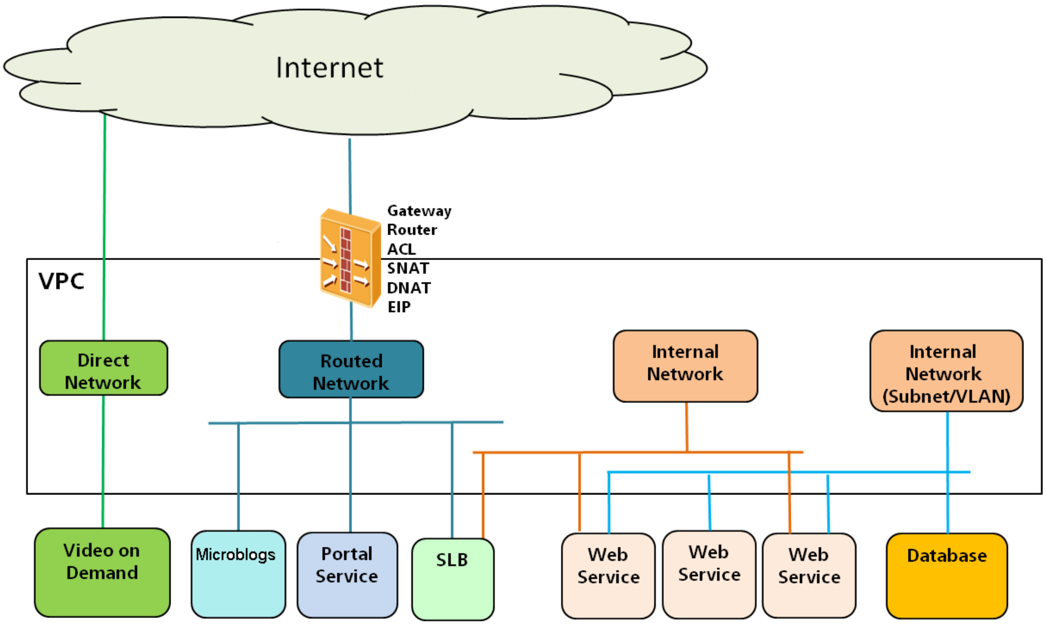
Description

In virtual data center solutions, network planes can be classified into the following types:

- Internal network: provides only VLANs and supports IP address management. An internal network provides only layer 2 networking capabilities. It is for internal use only and cannot communicate with external networks.
- Routed network: provides VLANs, IP address management functions, and layer 3 gateways. All routed networks in a VPC can communicate so that VMs on different

routed networks can access each other. Routes between gateways and virtual firewalls are created to allow the firewalls to protect VPCs.

- Direct network: connects a VM to an external network. All VMs on a direct network are assigned external IP addresses.
- External network: a network whose gateways and routes are not managed by the network plane of the virtual data center solution. An external network in the virtual data center solution is presented as an independent VLAN. The virtual data center does not control the IP address assignment for this VLAN.



Two IP address assignment modes are available for virtual data center solutions:

- DHCP: A software DHCP server is deployed in a VPC to assign IP addresses to VMs. The IP address assigned to a VM is fixed because IP addresses are bound to VMs in the virtual data center solution.
- Static injection: An IP address is specified for a VM when the VM is created. Due to the capability limitations of the virtualization layer, not all OSs support this IP address assignment mode.

VPCs use their own DHCP servers. Therefore, the same IP addresses can be assigned to multiple VPCs. End users can flexibly plan their internal addresses to resolve any issues that may arise.

To enable communication between departments, use the following method:

1. Plan a network segment for each VPC for global communication and then configure routers to implement communication.
2. Deploy an independent external network.

Enhancement

None

1.11.5.2 FSFD-080807 VPC Specifications Template

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

VPC Specifications Template defines the specifications of a VPC, including the number and bandwidths of networks.

Benefits

This feature facilitates statistics collection and VPC specifications management.

Description

VPC Specifications Template allows users to centrally manage VPC specifications in the system. Users can create, delete, modify, and query VPC specifications templates.

Enhancement

None

1.11.5.3 Multi-Tenant Support

1.11.5.4 FSFD-080901 VDC

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

Virtual Data Center (VDC) is a collection of virtual computing, storage, and network resources that are shared by VMs in this VDC.

Benefits

This feature allows users to perform the following operations:

- Create a virtual data center and deploy virtual clouds in it.
- Set resource quotas for the virtual data center to control its resource utilization.
- Lease the virtual data center to an enterprise.

Description

A VDC manages the CPU, memory, storage, and network resources available to an organization. This feature provides the following functions:

- Network device virtualization. The virtual data center technology virtualizes physical network devices, such as firewalls, load balancers, layer 2 and layer 3 network devices, DHCP servers, and VPN devices. End users can perform operations for these virtual devices the same way they configure physical devices.
- Organization resource isolation. The virtual data center technology allows resources allocated to different organizations to be isolated from each other so that IT personnel in each organization can independently use computing, storage, and network resources. The isolation simplifies configuration operations and enhances organization resource security.
- Resource allocation tracing. Virtual resources can be measured and managed based on the consumption volume.
- Self-service. The virtual data center technology simplifies IT systems and provides self-services, such as VM management and firewall configuration, on a unified management portal.

Enhancement

FusionSphere 3.1 supports network device automation. It supports virtualization of network devices, including firewalls, load balancers, layer 2 network devices, layer 3 gateways, DHCP servers, and VPN devices.

1.11.5.5 FSFD-080902 Tenant Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

Tenant Management allows FusionSphere to lease cloud platform resources to multiple tenants for them to deploy their own applications.

Benefits

This feature provides the following benefits for users:

- Resource sharing and independent resource use and management
- Multi-tenant operation
- On-demand resource use
- Improved resource utilization rates

Description

With Tenant Management, the cloud platform resources provided by FusionSphere can be leased to multiple tenants for them to deploy their own applications as required.

The resources allocated to different tenants are isolated, so that tenants can only query and manage their own resources. From the point of view of the entire FusionSphere system, the independently managed cloud resources are obtained from a shared resource pool on the cloud platform, which effectively provides cloud computing on-demand resource allocation.

Enhancement

None

1.11.6 Cloud Network Resource Pool Management

1.11.6.1 FSFD-081002 VLAN Resource Pool Management

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

VLAN Resource Pool Management defines which VLANs can be used by FusionSphere.

Benefits

This feature prevents VLAN conflicts among different application instances in the cloud system.

Description

This feature allows users to create, delete, modify, and query VLAN pools.

Enhancement

None

1.11.7 VM Template Services

1.11.7.1 FSFD-081301 VM Template Management

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

VM Template Management allows users to create VM templates, use existing templates on the virtualization platform to provision services, modify VM template attributes, and delete templates.

Benefits

This feature improves user experience for template management and service provisioning.

Description

Templates are used to create VMs and virtual application instances. This feature provides users with a unified platform for VM template management. On this platform, users can create VM templates or import templates from other hypervisors.

Enhancement

None

1.11.7.2 FSFD-081303 Secondary Storage

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

Secondary Storage allows users to add secondary storage for creating VM templates.

Benefits

This feature allows a VM template to be shared across the entire hypervisor platform.

Description

The virtualization platform supports unified secondary storage management. If a VM template or VM is stored in secondary storage, it can be shared across the entire platform, thereby implementing cross-cluster VM deployment.

Enhancement

None

1.11.7.3 FSFD-081304 Logical Template Management

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

Logical Template Management allows users to perform operations related to logical templates, including associating and disassociating VM templates and logical templates.

Benefits

This feature provides a unified platform for users to manage VM templates.

Description

Multiple VM templates can be associated with each logical template, so that users can manage and deploy logical templates on a unified platform.

Enhancement

None

1.11.8 Resource Pool Management

1.11.8.1 FSFD-081401Resource SLA

Availability

This feature was first available in FusionSphere 5.0 and requires a FusionSphere Advanced Edition license or above.

Summary

Resource SLA enables FusionSphere to allocate computing, storage, and network resources from proper resource pools to meet the requirements of different application instances or tenants.

Benefits

This feature enables users to properly plan and use virtual resources in resource pools.

Description

FusionSphere allows administrators to define different computing SLA levels for clusters by their computing performance, reliability requirement, or hardware models and for data stores by their storage media, reliability requirement, performance, or RAID levels. When a user applies for resources, FusionSphere allocates matched cluster and data store resources based on the requested computing and storage SLA levels.

Enhancement

None

1.11.8.2 FSFD-081402 Integrating Heterogeneous Virtual Resource Pools

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite advanced edition or above.

Summary

FusionManager supports hypervisors from various third-party vendors.

Benefits

This feature provides unified management and maintenance for hypervisors from different vendors, thereby cutting total cost of ownership (TCO).

Description

FusionManager supports centralized management of various hypervisors, including FusionCompute and VMware vSphere. In specific, FusionManager provides the following functions:

- Centrally manages data centers, hypervisors, and resource zones.
- Displays virtual resources, including the computing resource pool, storage resource pool, and network resource pool, in a unified manner.
- Allocates resources by organization or organization VDC.
- Manages deployed application instances.
- Supports southbound plug-ins for adding other virtualization platforms.

Managing Data Centers

The system administrator can divide the system into multiple data centers based on the system plan and manage the data centers. The system administrator can add, modify, delete, and query data centers. FusionManager can manage a maximum of 10 data centers.

Managing Resource Zones

In a data center, the resources that implement layer 2 communication on the service plane belong to a resource zone.

A resource zone is a logical resource collection that consists of hosts, data stores, elastic IP addresses, virtual firewalls (vFWs), and virtual load balancers (vLBs).

It is the largest resource group in a data center. Each resource zone has independent virtual local area networks (VLANs) and uplink ports. Resource zones are separated from each other on the layer 2 network. The VLANs for different resource zones may overlap.

The system administrator can add, modify, delete, and query resource zones. FusionManager can manage a maximum of 512 resource zones.

Managing Hypervisors

FusionManager can manage different types of hypervisors, such as FusionCompute, VMware vSphere.

The system administrator can add, delete, modify, query, and update hypervisors. FusionManager can manage a maximum of 256 hypervisors.

Enhancement

FusionSphere 5.1UI adds management over VMware vSphere 6.0.

1.12 Infrastructure Management

1.12.1 Infrastructure Management

1.12.1.1 FSFD-090104 Alarm Notification by Email or SMS

Availability

This feature was first available in FusionSphere 3.1 and requires a license of the virtualization suite advanced edition or above.

Summary

Alarm Notification by Email or SMS allows FusionSphere to connect to the email system or short message service (SMS) center and to send alarms to maintenance personnel by email or SMS.

Benefits

This feature enables maintenance personnel to receive alarm information at any time.

Description

FusionSphere supports the capability of sending alarms by email or SMS using the following methods:

- Connects to the email system and sends alarms to maintenance personnel by email through Simple Mail Transfer Protocol (SMTP).
- Connects to the SMS center and sends alarms to specified mobile devices by SMS.

Enhancement

None

1.12.2 Integrated Management

1.12.2.1 FSFD-090201Upgrade/Patching

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

Upgrade/Patching allows users to upgrade or patch the system.

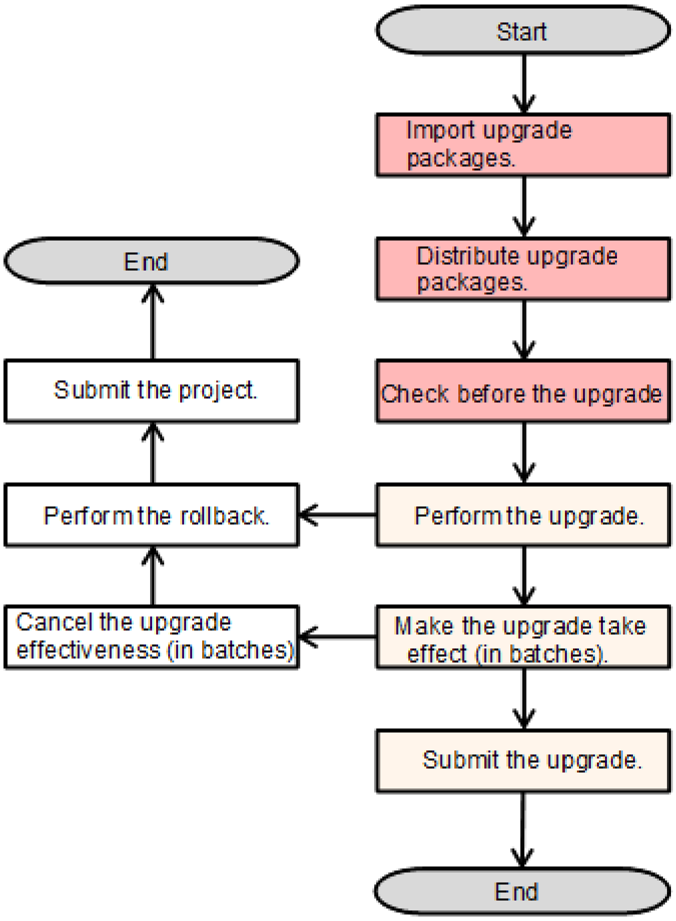
Benefits

This feature enables users to use new functions and helps users fix system bugs.

Description

Users can upgrade or patch the system using the upgrade tool. The following describes the upgrade process, and the patching process is similar to the upgrade process:

- **Preparations before the upgrade:** includes importing upgrade packages, distributing upgrade packages, and check before the upgrade. The preparations are required to be completed three days to half an hour before the upgrade. These operations have no adverse impact on the system.
- **Upgrade:** includes performing the upgrade, making the upgrade take effect, and submitting the upgrade. The first two steps are typically performed on the current day of the upgrade, whereas the last submitting step is performed one week after the upgrade takes effect. If any exception is detected within this week, the system can be rolled back. The fast upgrade and online upgrade modes are available. The fast upgrade interrupts VM services, whereas the online upgrade is performed in service.
- **Rollback:** includes canceling the upgrade effectiveness, performing the rollback, and submitting the project. A rollback is required if the upgrade fails or service exceptions occur after the upgrade takes effect. The fast rollback and online rollback modes are available.



Enhancement

None

1.12.2.2 FSFD-090202 Information Collection Tool

Availability

This feature was first available in FusionSphere 3.0 and requires a license of the virtualization suite standard edition or above.

Summary

FusionSphere provides an information collection tool that automatically collects system logs based on the specified node, log type, time period, and log level.

Benefits

This feature allows users to quickly locate and analyze faults.

Description

The information collection tool automatically collects system logs based on the specified node, log type, time period, and log level.

Enhancement

Added information collection for the host OS serial ports and Kbox as well as VM serial ports and Kbox.

1.12.2.3 FSFD-090203 Health Check Tool

Availability

This feature was first available in FusionSphere 5.0 and requires a license of the virtualization suite standard edition or above.

Summary

FusionSphere provides a health check tool that checks the health status of FusionCompute and FusionManager.

Benefits

This feature allows customers to perform daily, weekly, monthly, quarterly, and yearly preventive maintenance and therefore identify hidden risks in a timely manner.

Description

The health check tool provides the following functions:

- Provides a web UI for users, supports automatic installation and uninstallation, and supports real-time and periodic preventive maintenance.
- Supports customization of preventive maintenance nodes and check items.
- Supports preventive maintenance for desktop servers, cloud management platforms, and infrastructure platforms.
- Provides a wizard for fault rectification.
- Automatically generates preventive maintenance reports.

Enhancement

Added some health check items for FusionSphere OpenStack.

1.13 VM Migration from Other Hypervisors to VRM

1.13.1 FSFD-012301 Automatic Migration

Availability

This feature was first available in Rainbow2.0.

Summary

Rainbow provides a wizard for migrating VMs from VMware, Xen, and KVM hypervisors to FusionCompute. Only four steps are required for completing a migration task.

Benefits

This feature simplifies migration operations, reduces man-made mistakes, and improves migration efficiency. A migration task can be completed within 1 minute.

Description

The automatic migration task is created on the Rainbow wizard. The task includes the following steps:

1. Automatic VM specifications planning before the migration
2. Automatic VM creation before the migration
3. Automatic installation package push before the migration
4. Automatic IP address setting before the migrationThe entire operation procedure takes about 1 minute.

Impact on the System

None

Application Limitations

Only online migration is supported.

This feature has the following constraints:

- Hardware: This feature supports only OEM OSs. The OSs or applications, such as dongle, are bound with the hardware.
- Virtualization: This feature supports paravirtualized VMs.
- File system: This feature supports encrypted file systems. It does not support migration of bare metal servers. In Windows OSs, it supports non-NTFSs; in Linux OSs, it supports files systems other than EXT2, EXT3, EXT4, REISERFS, XFS, and VFAT.
- Application: If the system contains cluster applications, for example, DB, AD, and Email system, you are advised to use the migration plans offered by the applications.

Application scope: This feature does not support migration in FusionAccess and public cloud scenarios.

Network: The live network must ensure the ICMP connectivity among the source, destination, and three Rainbow nodes. The ports must meet requirements in the migration port matrix.

Feature Interactions

None

Technical Description

1. The user logs in to the server with the Rainbow migration tool installed and creates a migration task.
2. The user enters the credentials of the source host for authentication.
3. The tool server automatically deploys the migration agent, prepares the VMs on the destination host, and verifies the network connectivity.
    1) The tool server pushes the source agent to the source host, starts the host, and reports the specifications of the source host.
    2) The tool server makes a call to the FusionSphere API to create VMs with the same specifications as those on the source host.
    3) The tool server calls the DVD-ROM drive loading API and IP address setting API to load the destination agent from the DVD-ROM drive, set IP addresses, and run the agent program.
    4) The destination agent partitions and formats VMs.
    5) The tool server, source agent, and destination agent authenticate one another.
4. The source agent creates system and data volume snapshots and reads snapshot files as blocks or files.
5. The Windows or Linux transmission component performs data migration.
6. The destination agent receives data, writes data to the local system and data volumes, and completes driver adaptation.
7. The tool unmounts the DVD-ROM drive and releases the destination agent.
8. The VM boots from the system volumes, and the PV driver is automatically installed on the VM. The migration is complete.

Specifications

Duration for a single migration task: 4 steps within 1 minute

Enhancement

None

Reference

None

1.13.2 FSFD-012303 Windows Migration

Availability

This feature was first available in Rainbow1.0.

Summary

Rainbow supports Windows OS migration from VMware, Xen, and KVM hypervisors to FusionCompute by file or block.

Benefits

Rainbow offers users with two migration methods which apply to various migration scenarios.

Description

File-level Windows OS migration copies OS files from the source VM to the destination VM.

Block-level Windows OS migration copies data blocks on valid sector of disks from the source VM to the destination VM.

Impact on the System

None

Application Limitations

This feature has the following constraints:

- Hardware: This feature supports only OEM OSs. The OSs or applications, such as dongle, are bound with the hardware.
- Virtualization: This feature supports paravirtualized VMs.
- File system: This feature supports encrypted file systems. It does not support migration of bare metal servers. In Windows OSs, it supports non-NTFSs.
- Application: If the system contains cluster applications, for example, DB, AD, and Email system, you are advised to use the migration plans offered by the applications.

Feature Interactions

None

Technical Description

None

Specifications

None

Enhancement

None

Reference

None

1.13.3 FSFD-012304 Linux Migration

Availability

This feature was first available in Rainbow1.0.

Summary

Rainbow supports Linux OS migration from VMware, Xen, and KVM hypervisors to FusionCompute by file or block.

Benefits

Rainbow offers users with two migration methods which apply to various migration scenarios.

Description

File-level Linux OS migration copies OS files from the source VM to the destination VM.

Block-level Linux OS migration copies data blocks on all sectors of disks from the source VM to the destination VM.

Impact on the System

None

Application Limitations

This feature has the following constraints:

- Hardware: This feature supports only OEM OSs. The OSs or applications, such as dongle, are bound with the hardware.
- Virtualization: This feature supports paravirtualized VMs.

- File system: This feature supports encrypted file systems. It does not support migration of bare metal servers. In Windows OSs, it supports non-NTFSs. In Linux OSs, it supports files systems other than EXT2, EXT3, EXT4, REISERFS, XFS, and VFAT.
- Application: If the system contains cluster applications, for example, DB, AD, and Email system, you are advised to use the migration plans offered by the applications.

Feature Interactions

None

Technical Description

None

Specifications

None

Enhancement

None

Reference

None

1.13.4 FSFD-012305 Offline Data Synchronization

Availability

This feature was first available in Rainbow2.0.

Summary

Offline Data Synchronization enables new data to be synchronized to the destination VMs after the migration is complete.

Benefits

This feature helps customers to synchronize changed data to the destination VM after the VM migration and before service cutover.

Description

This feature compares files between source and destination VMs and copies the changed files from the source to the destination, thereby synchronizing data.

Impact on the System

None

Application Limitations

None

Feature Interactions

None

Technical Description

None

Specifications

Data migration of incremental services is implemented based on file comparison, and therefore the migration efficiency is low.

Enhancement

None

Reference

None

1.13.5 FSFD-012306 Concurrent Migration Tasks

Availability

This feature was first available in Rainbow1.0.

Summary

Rainbow supports concurrent migration tasks.

Benefits

This feature improves migration efficiency and shortens the time required for migration delivery.

Description

Rainbow supports multiple migration or synchronization tasks in progress, and these tasks exert no adverse impacts on one another.

Impact on the System

None

Application Limitations

None

Feature Interactions

None

Technical Description

None

Specifications

Up to 30 migration tasks can be concurrently performed.

Enhancement

None

Reference

None

1.13.6 FSFD-012307 Log Collection

Availability

This feature was first available in Rainbow1.0.

Summary

Rainbow collects logs generated in the migration process.

Benefits

This feature helps customers easily locate faults that may occur during the migration process.

Description

Users can export logs on the Rainbow page, including source agent logs, destination agent logs, and the logs generated by Rainbow on the migration server.

Impact on the System

None

Application Limitations

None

Feature Interactions

None

Technical Description

None

Specifications

None

Enhancement

None

Reference

None

1.13.7 FSFD-012308 Support for Guest OSs

Availability

This feature was first available in Rainbow1.0.

Summary

- Rainbow supports mainstream OSs.
- Rainbow supports mainstream virtualization platforms and x86 servers.

Benefits

Rainbow applies to most of the migration scenarios.

Description

- Support for more than 160 types of OSs

In an online migration, the source end supports the OSs listed in the following table, whereas UEFI supports only the migration to FusionCompute V100R005C10/V100R006C00.

For details about supported guest OSs, use Huawei FusionCloud Compatibility Check Assistant. The link of obtaining this tool is as follows:

http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.en.jsp

- Support for mainstream virtualization platforms and x86 servers

The following table lists supported source virtualization platforms for online migration.

Source Virtualization Platform	Destination FusionSphere Version
VMware vSphere 4.1 VMware vSphere 5.0 VMware vSphere 5.1 VMware vSphere 5.5 VMware vSphere 6.0 Citrix XenServer 6.0 (fully virtualized VMs) Red Hat Enterprise Linux 6.2 KVM Red Hat Enterprise Linux 7.0 KVM Red Hat Enterprise Linux 7.1 KVM Hyper-V 2008/2008 R2 Hyper-V 2012/2012 R2 SUSE11 XEN X86 servers of mainstream vendors, such as HP, Dell, and IBM.	FusionCompute V100R003C00 FusionCompute V100R003C10 FusionCompute V100R005C00 FusionCompute V100R005C10 FusionCompute V100R006C00

Impact on the System

None

Application Limitations

None

Feature Interactions

None

Technical Description

None

Specifications

None

Enhancement

None

Reference

None

A Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
ACL	access control list
API	application programming interface
ARP	Address Resolution Protocol
ASPF	Application Specific Packet Filter
BMC	baseboard management controller
CAD	computer aided design
CAE	computer aided engineering
CAM	computer aided manufacturing
CBT	Changed Block Tracking
CIFS	common internet file system
CNA	Computing Node Agent
CPU	central processing unit
DHCP	Dynamic Host Configuration Protocol
DMA	direct memory access
Dom0	Domain 0
DPM	dynamic power management
DRS	dynamic resource scheduler
ECC	error checking and correction
eTOM	enhanced Telecom Operations Map
EVS	elastic virtual switch
FC SAN	fiber channel storage area network

Acronym and Abbreviation	Full Name
FTP	File Transfer Protocol
GDI	graphics device interface
GPU	graphic processing unit
HA	high availability
HBA	host bus adapter
IaaS	Infrastructure as a Service
I/O	input and output
IOMMU	input/output memory management unit
IP SAN	IP storage area network
IPsec	Internet Protocol Security
iSCSI	Internet Small Computer System Interface
ISO	International Organization for Standardization
L2TP	Layer 2 Tunneling Protocol
LUN	logical unit number
MAC	Media Access Control
MMIO	Memory Mapping I/O
MTU	maximum transmission unit
NAPT	Network Address Port Translation
NAS	network attached storage
NAT	Network Address Translation
NFS	network file system
NTP	Network Time Protocol
NUMA	non-uniform memory access
NVDIMM	non-volatile dual in-line memory module
PKI	public key infrastructure
PVSCSI	paravirtual SCSI
QoS	quality of service
RAC	Real Application Clusters
RAID	Redundant Array of Independent Disks
RDM	raw device mapping

Acronym and Abbreviation	Full Name
RPO	recovery point object
RTO	recovery time object
SAN	storage area network
SCSI	Small Computer Systems Interface
SMP	symmetric multiprocessing
SNAT	Source Network Address Translation
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SR-IOV	single root i/o virtualization
SSH	Secure Shell
TC	thin client
TCP	Transmission Control Protocol
TOR	Top of Rack
UDS	Universal Distributed Storage
USB	Universal Serial Bus
UVP	Unified Virtualization Platform
VDC	virtual data center
vFW	virtual firewall
VGA	video graphics array
VIMS	Virtual Image Management System
VLAN	virtual local area network
vLB	virtual load balancer
VM	virtual machine
VMDq	Virtual Machine Device Queues
VNC	Virtual Network Computing
vNIC	virtual network interface card
VPC	virtual private cloud
VPN	virtual private network
VSP	virtual switch port
VSS	Volume Shadow copy Service

Acronym and Abbreviation	Full Name
VXLAN	virtual extensible local area network
VXLAN VTEP	VXLAN Tunnel Endpoints