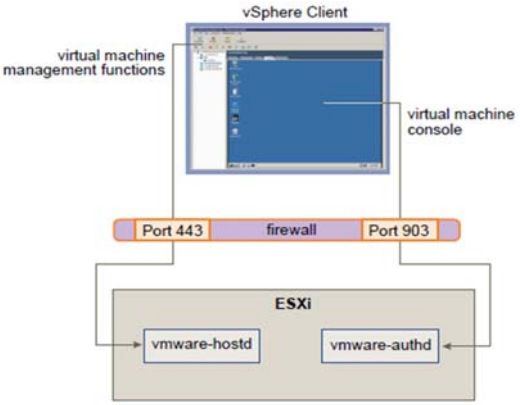
VMware Management Availability, Security

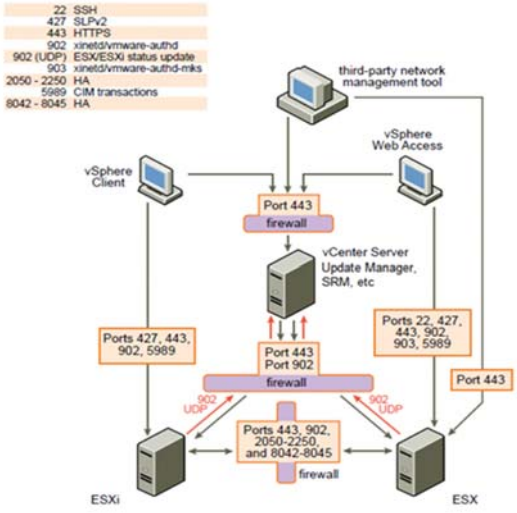
Tien-Fu Chen

Dept. of Computer Science
National Chiao Tung Univ.

Management Network

- The entire management LAN is isolated from other LAN
- Within the Management LAN, put a firewall between:
  - ESXi and vCenter
  - vSphere Client and ESXi/vCenter.
  - No need firewall among ESXi.





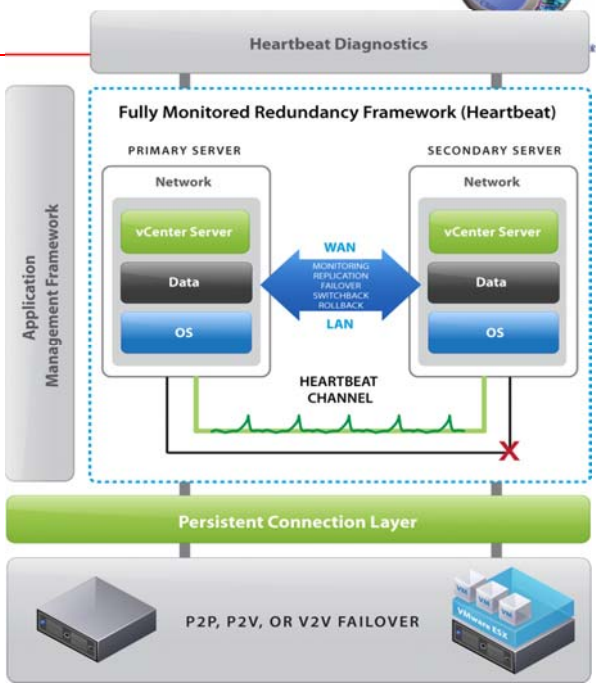
vCenter

- Run vCenter Server as a VM
  - vCenter Server VM best practices:
    - Disable DRS on this VM. Move VC to first ESXi on your farm.
    - Always remember where you run your vCenter.
    - Remember both the host name and IP address of that first ESXi host.
  - Start in this order: Active Directory → DNS → vCenter DB → vCenter
    - Set HA to high priority
  - Limitations
    - Windows patching of vCenter VM can't be done via Update Manager
    - Can't cold clone the VM. Use hot clone instead.
    - VM-level operation that requires the VM to be powered-off, can be done via ESX.
      - Login directly to the ESXi host that has the vCenter VM. Do the changes, then boot the VM.
  - Not connected to Production LAN. Connect to management LAN, so VLAN Trunking required as vSwitches are shared (assuming you are not having dedicated IT Cluster)
- Security
  - Protect the special-purpose local vSphere administrator account from regular usage. Instead, rely on accounts tied to specific individuals for clearer accountability.

vCenter Server: HA

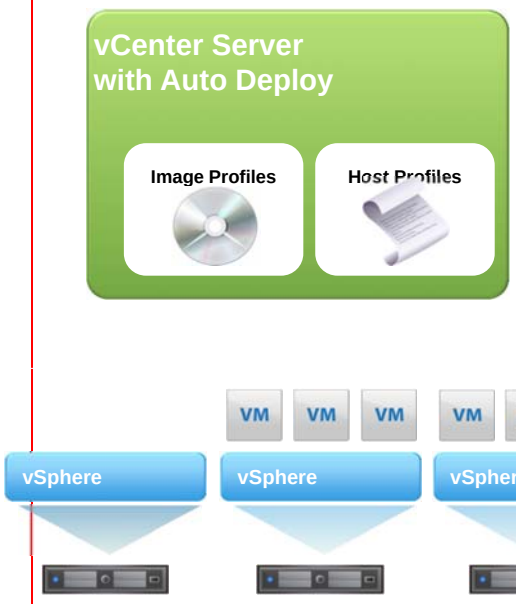
Many vSphere features depend on vCenter
- Distributed Switch
- Auto-Deploy
- HA (management)
- DRS and vMotion
- Storage vMotion
- Licensing

Many add-on depends on vCenter
- vShield
- vCenter SRM
- VCM
- vCenter Operations
- vCenter Chargeback
- vCloud Director
- View + Composer



Implement vCenter Heartbeat
- Automated recovery from hardware, OS, application, network
- Awareness of all vCenter Server components
- Only solution fully supported by VMware
- Can protect database (SQL Server) and vCenter plug-ins

vCenter Server with Auto Deploy



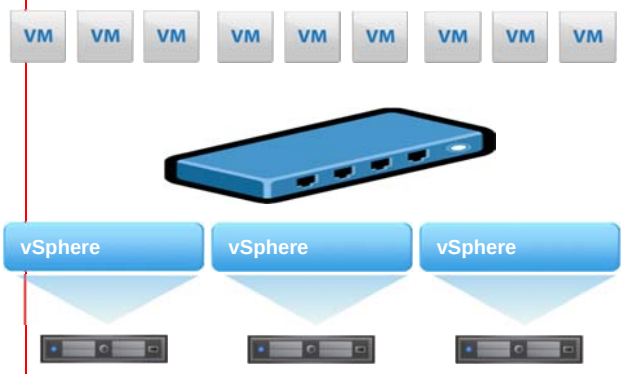
Overview

- Deploy and patch vSphere hosts in minutes using a new “on the fly” model
- Coordination with vSphere Host Profiles
- 2 new operating modes

Benefits

- Fast initial deployment and patching
- Centralized host and image management
- Reduce manual deployment and patch processes
- Continue deployment even when a failure occurs

Distributed Switch



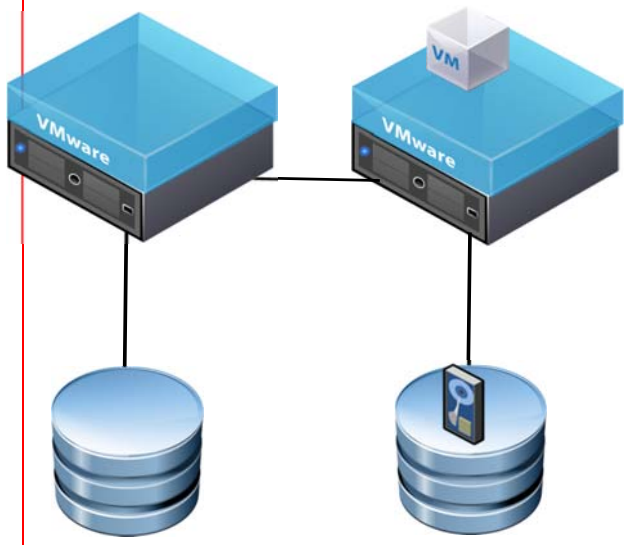
Overview

- Distributed Switch now delivers:
  - Network Healthcheck
  - Configuration Backup and Restore
  - Roll Back and Recovery
  - LACP Support

Benefits

- Visibility into physical and virtual network status
- Backup and recover network settings
- Fast recovery from lost connectivity or incorrect configurations

vMotion (w/o Shared Storage)



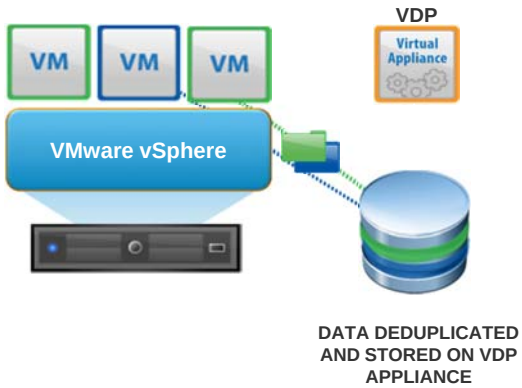
Overview

- Live migration of a virtual machine without the need for shared storage
- Extends VMware's revolutionary technology for automated virtual machine movement

Benefits

- Zero downtime migration
- No dependency on shared storage
- Lower operating cost
- Helps meet service level and performance SLAs

vSphere Data Protection



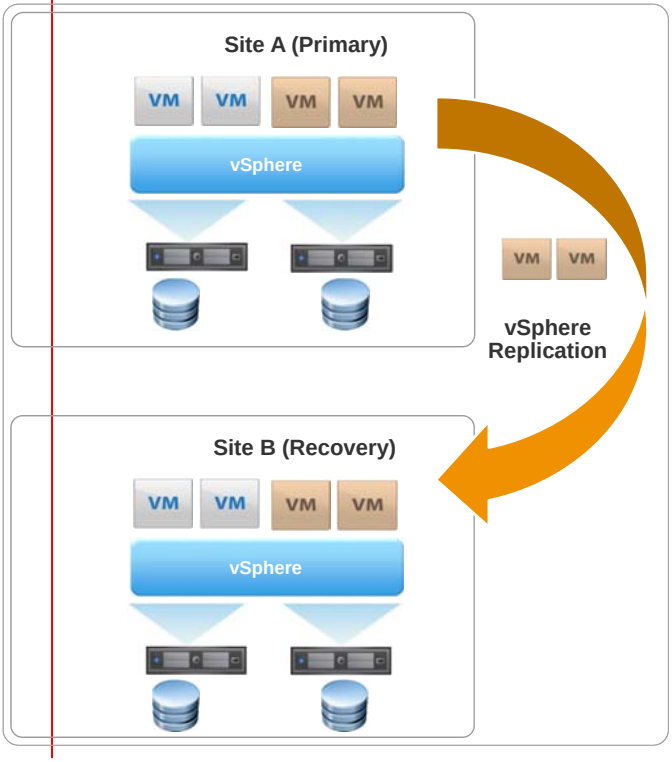
Overview

- New backup and recovery tool for the vSphere platform
- Replaces vSphere Data Recovery
- Based on EMC Avamar

Benefits

- Use less disk space with deduplication
- Simple setup and management
- Proven technology

vSphere Replication



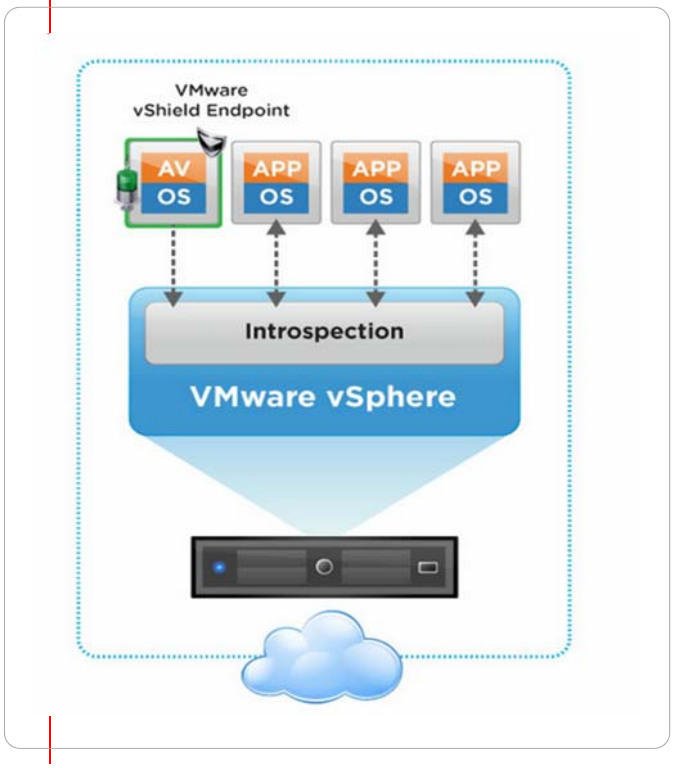
Overview

- Virtual machine level replication by the vSphere host
- Included with vSphere*

Benefits

- Low cost/efficient replication option
- Simple setup from within vCenter Server
- Integration with SRM enables automated DR process

vShield Endpoint



Overview

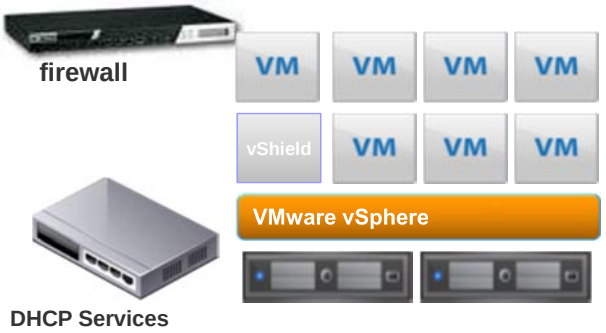
- Secure your VMs with offloaded anti-virus and anti-malware (AV) solutions without the need of agents
- Included with vSphere*

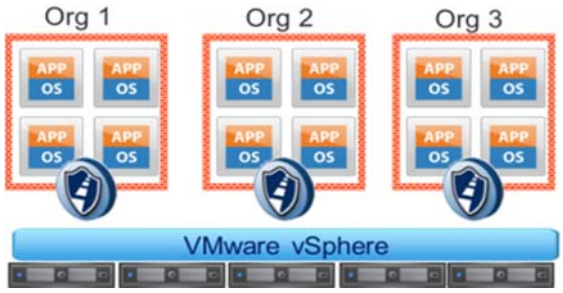
Benefits

- Simplified AV administration
- Higher consolidation ratios by preventing the possibility of AV storms
- Improved performance

Integrated vShield features simplify security and compliance

- vShield for vCloud Director is a virtual appliance providing essential perimeter network and security services including:
  - Port-level stateful firewall
  - Network Address Translation
  - DHCP services
- Enables fast, secure and automated provisioning of multitenant Org VDCs in private clouds
  - Simpler, easer to operate
    - One Edge per Org, deployed anywhere
    - Built-in network isolation
    - Integrated and manageable by REST APIs for script and 3rd party automation
  - Improved visibility, control and compliance
    - Application aware NetFlow visibility
    - Automated log collection with syslog and VC integration





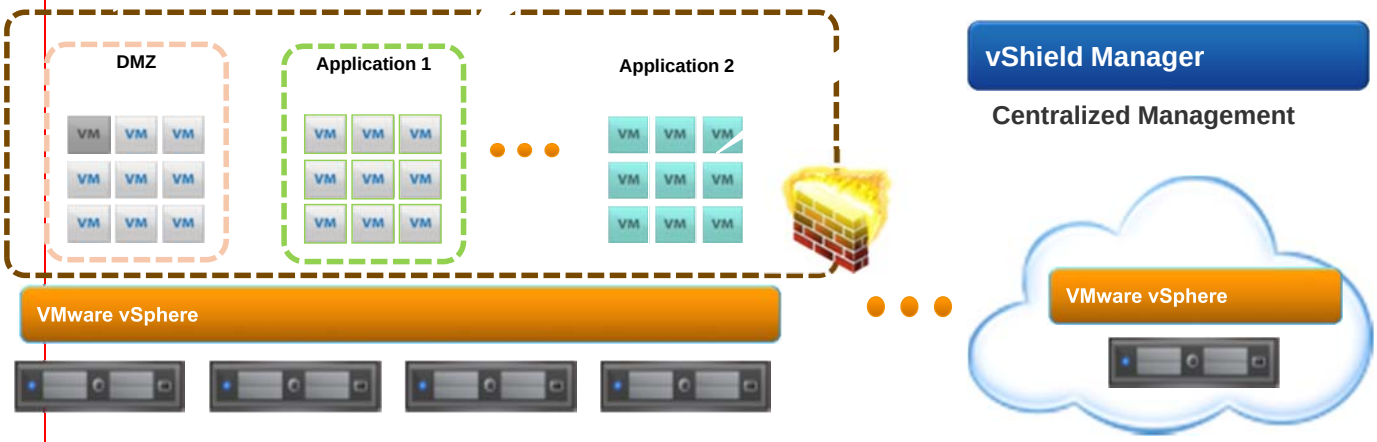
vShield

Security from Edge to Endpoint

vShield Edge
Secure the edge of the virtual datacenter

vShield App
Application protection from network-based threats

vShield Endpoint
Offload anti-virus processing



Storage Virtualization and VMware Solutions

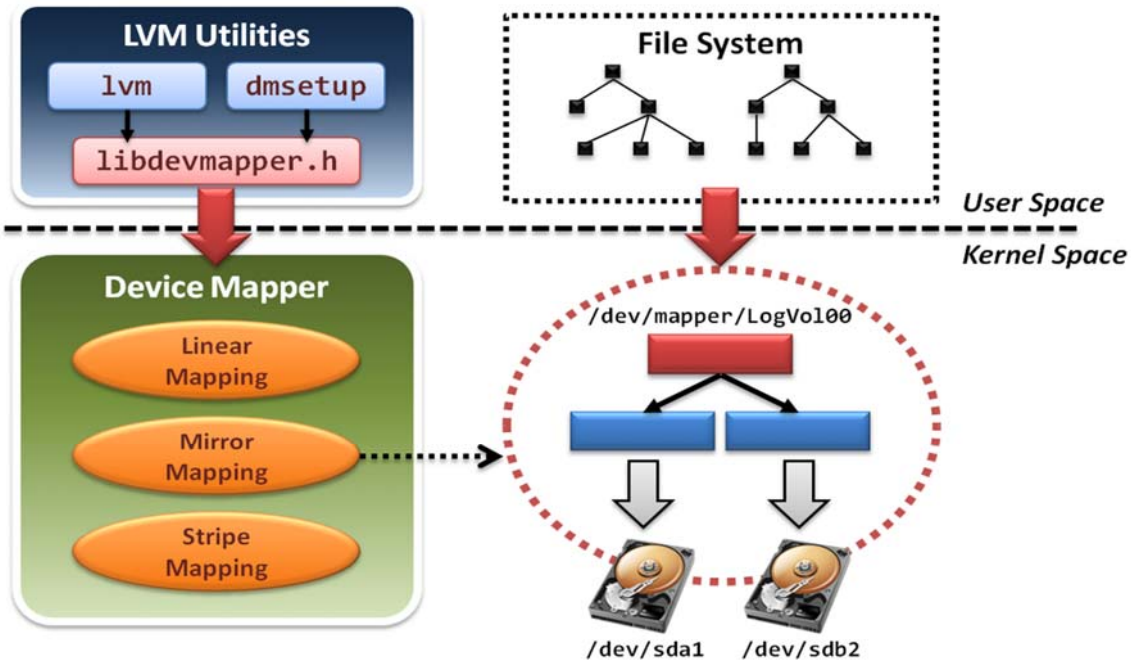
Tien-Fu Chen

Dept. of Computer Science
National Chiao Tung Univ.

Source: NTHU courses
Virtualization and cloud computing

Logical Volume Management in Linux

- LVM architecture

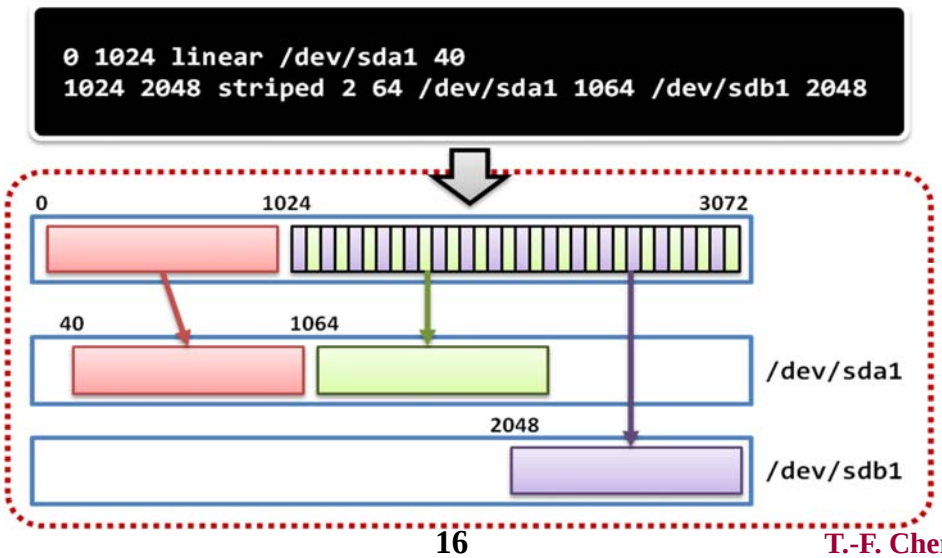


Logical Volume Management

- **lvm**
  - Command-line tools for LVM2.
    - logical volume (**lv**) operations
    - volume group (**vg**) operations
    - physical volume (**pv**) operations
  - Limited controllability
    - Only can create logical volume with simple mapping mechanisms.
    - Do not allow cross machine mappings.
- **dmsetup**
  - Limitations
    - Still cannot provide cross machine mappings.

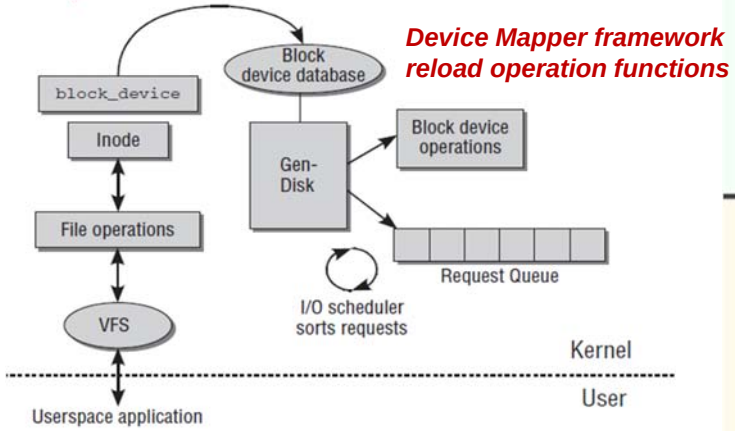
Logical Volume Management

- **dmsetup**
  - low level logical volume management
    - Operate create, delete, suspend and resume …etc
    - Work with mapping table file

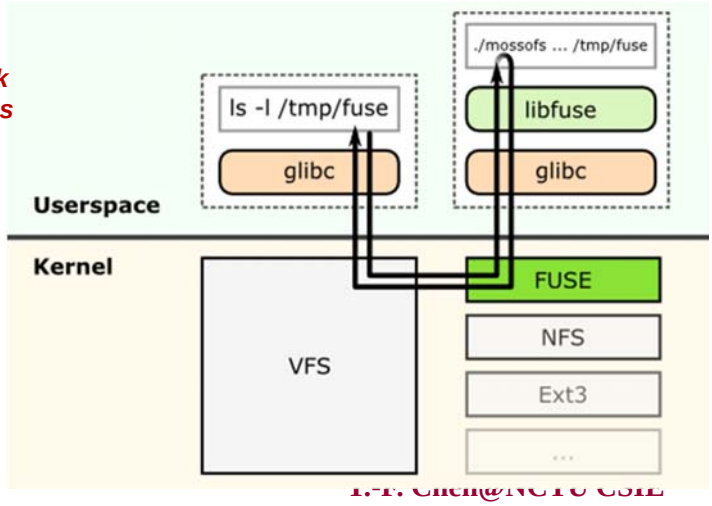


Logical Volume Management

- File system in operating system will invoke a set of block device system calls.
- File system can be also implemented in the user space only.



Device Mapper framework reload operation functions

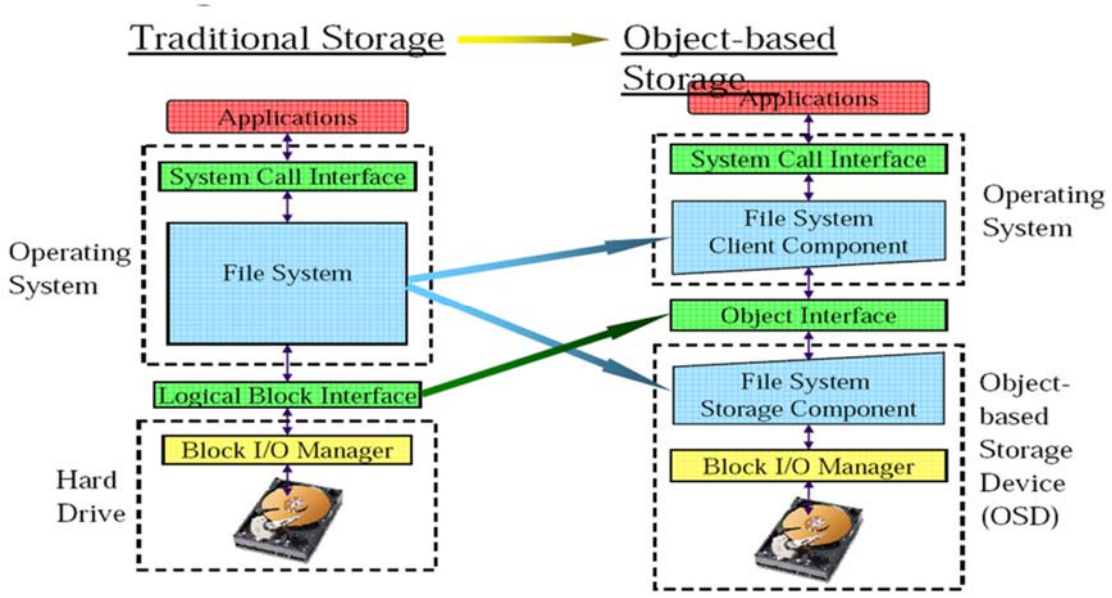


Ceph

- **Overview**
  - Ceph is a free software distributed file system.
  - Ceph's main goals are to be POSIX-compatible, and completely distributed without a single point of failure.
  - The data is seamlessly replicated, making it fault tolerant.
- Features
  - Ceph is a distributed file system that provides excellent performance ,reliability and scalability.
  - Objected-based Storage.
  - Ceph separates data and metadata operations by eliminating file allocation tables and replacing them with generating functions.
  - Ceph utilizes a highly adaptive distributed metadata cluster, improving scalability.
  - Using object-based storage device (OSD) to directly access data, high performance.

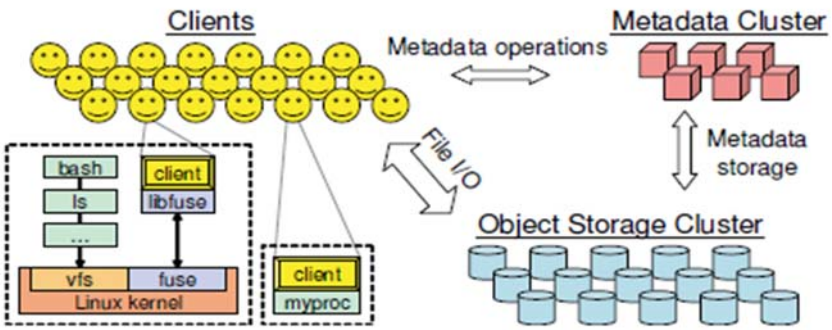
Ceph

- Objected-Based Storage



Ceph

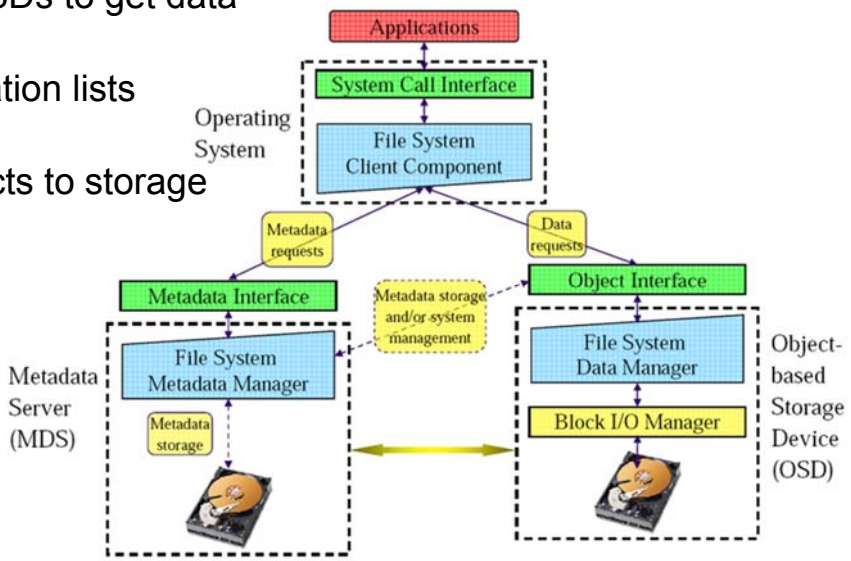
- Three main components
  - Clients : Near-POSIX file system interface.
  - Cluster of OSDs : Store all data and metadata.
  - Metadata server cluster : Manage namespace (file name).



Three Fundamental Design

1. Separating Data and Metadata

- Separation of file metadata management from the storage.
- Metadata operations are collectively managed by a metadata server cluster.
- User can direct access OSDs to get data by metadata.
- Ceph removed data allocation lists entirely.
- Usr CRUSH assigns objects to storage devices.



Dynamic Distributed Metadata Management

2. Dynamic Distributed Metadata Management

- Ceph utilizes a metadata cluster architecture based on Dynamic Subtree Partitioning.(workload balance)

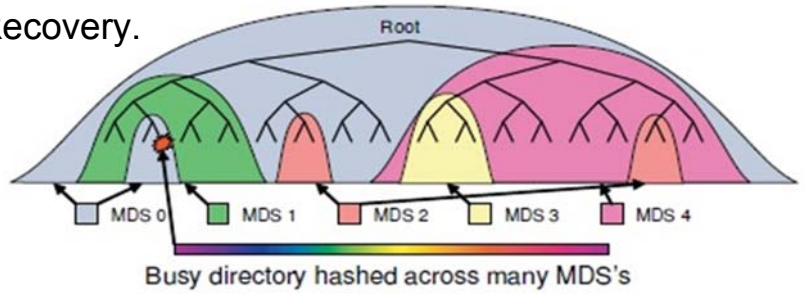
– Dynamic Subtree Partitioning

- Most FS ,use static subtree partitioning
  →imbalance workloads.
  →simple hash function can get directory.
- Ceph's MDS cluster is based on a dynamic subtree partitioning.
  →balance workloads

3. Reliable Autonomic Distributed Object Storage

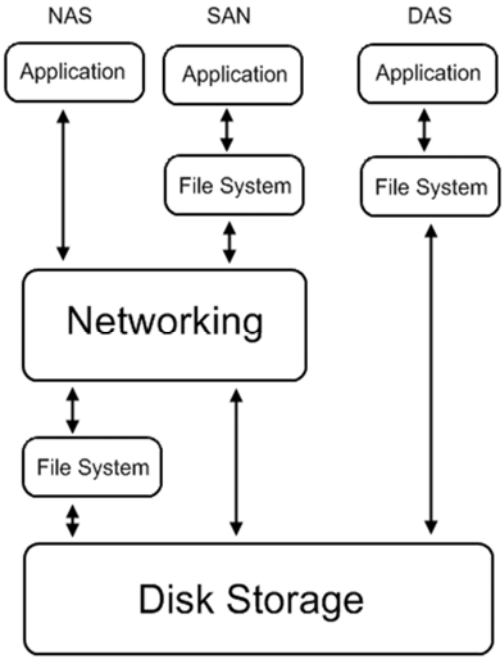
– Replica.

– Failure Detection and Recovery.



Introduction
Storage Virtualization

- Common storage architecture :
  - DAS - Direct Attached Storage
    - Storage device was directly attached to a server or workstation, without a storage network in between.
  - NAS - Network Attached Storage
    - File-level computer data storage connected to a computer network providing data access to heterogeneous clients.
  - SAN - Storage Area Network
    - Attach remote storage devices to servers in such a way that the devices appear as locally attached to the operating system.

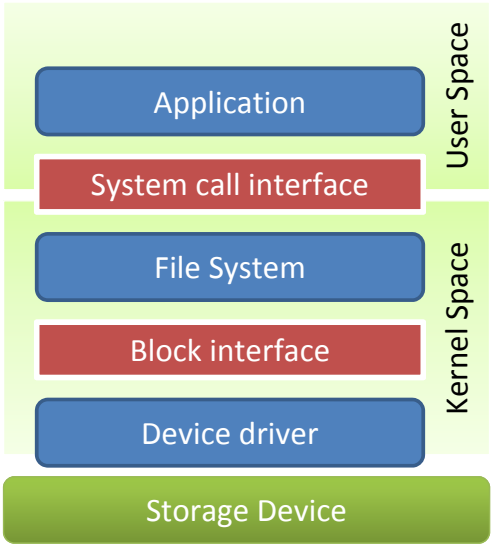


Introduction

- Desirable properties of storage virtualization:
  - Manageability
    - Storage resource should be easily configured and deployed.
  - Availability
    - Storage hardware failures should not affect the application.
  - Scalability
    - Storage resource can easily scale up and down.
  - Security
    - Storage resource should be securely isolated.

What To Be Virtualized

- Layers can be virtualized
  - File system
    - Provide compatible system call interface to user space applications.
  - Block device
    - Provide compatible block device interface to file system.
    - Through the interface such as SCSI, SAS, ATA, SATA, etc.



File System Level

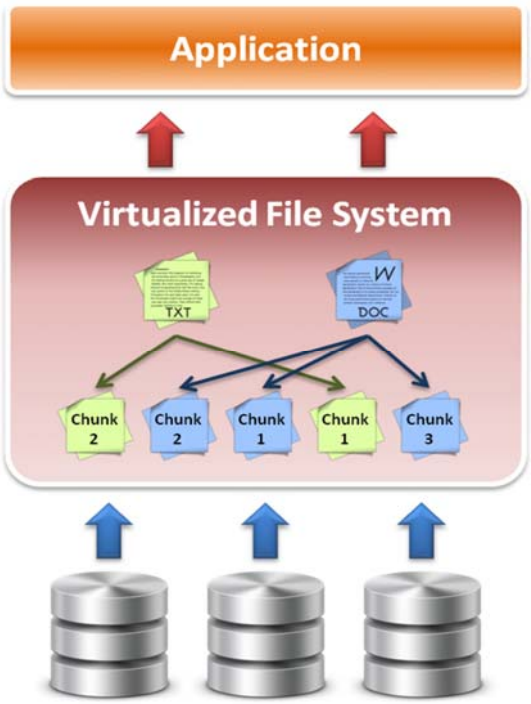
- Data and Files
  - What is data ?
    - Data is information that has been converted to a machine-readable, digital binary format.
    - Control information indicates how data should be processed.
    - Applications may embed control information in user data for formatting or presentation.
    - Data and its associated control information is organized into discrete units as files or records.
  - What is file ?
    - Files are the common containers for user data, application code, and operating system executables and parameters.

File System Level

- File system
  - What is file system ?
    - A file system is a software layer responsible for organizing and policing the creation, modification, and deletion of files.
    - File systems provide a hierarchical organization of files into directories and subdirectories.
    - The *B*-tree algorithm facilitates more rapid search and retrieval of files by name.
    - File system integrity is maintained through duplication of master tables, change logs, and immediate writes off file changes.
  - Different file systems
    - In Unix, the super block contains information on the current state of the file system and its resources.
    - In Windows NTFS, the master file table contains information on all file entries and status.

File System Level

- File system level virtualization
  - File system maintains metadata (*i*-node) of each file.
  - Translate file access requests to underlining file system.
  - Sometime divide large file into small sub-files (chunks) for parallel access, which improves the performance

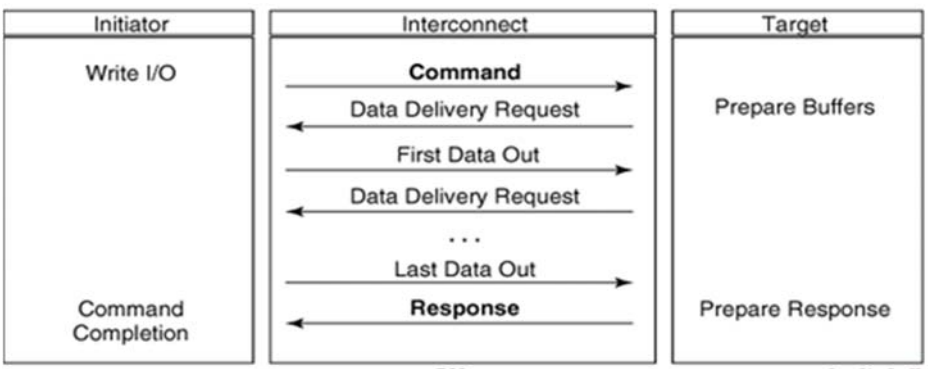


Block Device Level

- Block level data
  - The file system block
    - The atomic unit of file system management is the file system block.
    - A file's data may span multiple file system blocks.
    - A file system block is composed of a consecutive range of disk block addresses.
  - Data in disk
    - Disk drives read and write data to media through cylinder, head, and sector geometry.
    - Microcode on a disk translates between disk block numbers and cylinder/head/sector locations.
    - This translation is an elementary form of virtualization.

Block Device Level

- Block device interface
  - SCSI (*Small Computer System Interface*)
    - The exchange of data blocks between the host system and storage is governed by the SCSI protocol.
    - The SCSI protocol is implemented in a client/server model.
    - The SCSI protocol is responsible for block exchange but does not define how data blocks will be placed on disk.
    - Multiple instances of SCSI client/server sessions may run concurrently between a server and storage.

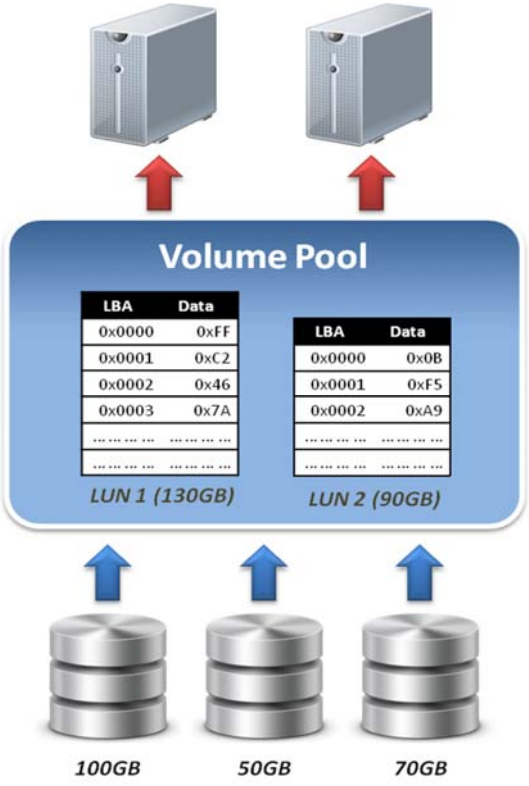


Block Device Level

- Logical unit and Logical volume
  - Logical unit
    - The SCSI command processing entity within the storage target represents a logical unit (LU) and is assigned a logical unit number (LUN) for identification by the host platform.
    - LUN assignment can be manipulated through LUN mapping, which substitutes virtual LUN numbers for actual ones.
  - Logical volume
    - A volume represents the storage capacity of one or more disk drives.
    - Logical volume management may sit between the file system and the device drivers that control system I/O.
    - Volume management is responsible for creating and maintaining metadata about storage capacity.
    - Volumes are an archetypal form of storage virtualization.

Block Device Level

- Data block level virtualization
  - LUN & LBA
    - A single block of information is addressed using a logical unit identifier (LUN) and an offset within that LUN, which known as a Logical Block Address (LBA).
  - Apply address space remapping
    - The address space mapping is between a logical disk and a logical unit presented by one or more storage controllers.

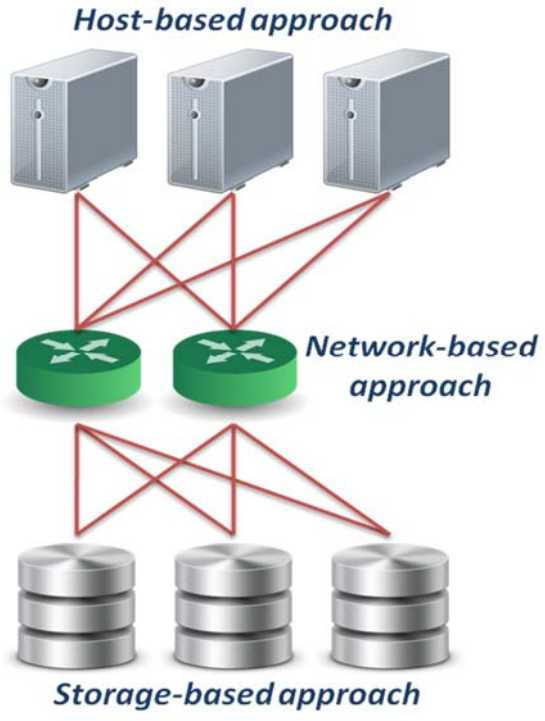


Where To Be Virtualized

- Storage interconnection protocol
  - Fibre Channel
    - Usually for high performance requirements.
    - Supports point-to-point, arbitrated loop, and fabric interconnects.
    - Device discovery is provided by the simple name server (SNS).
    - Fibre Channel fabrics are self-configuring via fabric protocols.
  - iSCSI (*internet SCSI*)
    - For moderate performance requirements.
    - Encapsulates SCSI commands, status and data in TCP/IP.
    - Device discovery by the Internet Storage Name Service (iSNS).
    - iSCSI servers can be integrated into Fibre Channel SANs through IP storage routers.

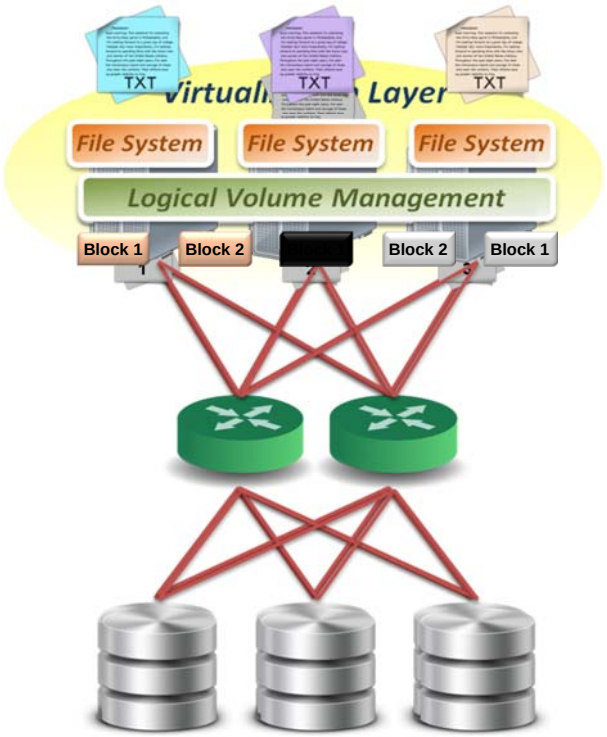
Where To Be Virtualized

- Different approaches :
  - Host-based approach
    - Implemented as a software running on host systems.
  - Network-based approach
    - Implemented on network devices.
  - Storage-based approach
    - Implemented on storage target subsystem.



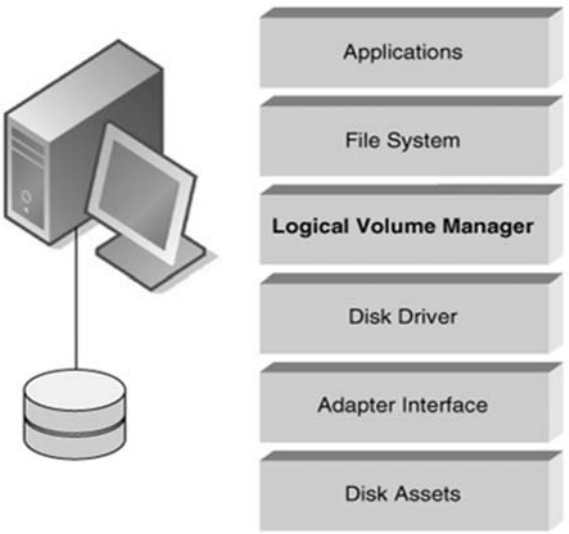
Host-based Virtualization

- Host-based approach
  - File level
    - Run virtualized file system on the host to map files into data blocks, which distributed among several storage devices.
  - Block level
    - Run logical volume management software on the host to intercept I/O requests and redirect them to storage devices.
  - Provide services
    - Software RAID



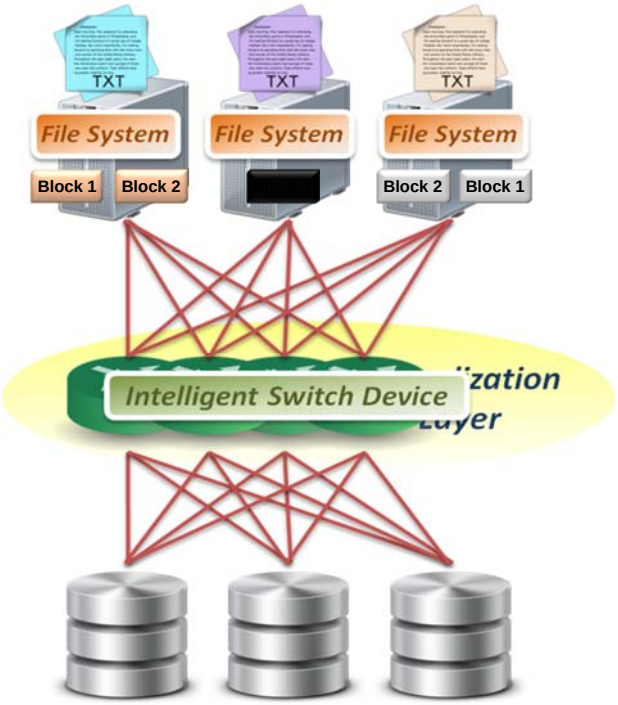
Host-based Virtualization

- A typical example :
  - LVM
    - Software layer between the file system and the disk driver.
    - Executed by the host CPU.
    - Lack hardware-assist for functions such as software RAID.
    - Independence from vendor-specific storage architectures.
    - Dynamic capacity allocation to expand or shrink volumes.
    - Support alternate pathing for high availability.



Network-based Virtualization

- Network-based approach
  - File level
    - Seldom implement file level virtualization on network device.
  - Block level
    - Run software on dedicated appliances or intelligent switches and routers.
  - Provide services
    - Multi-path
    - Storage pooling

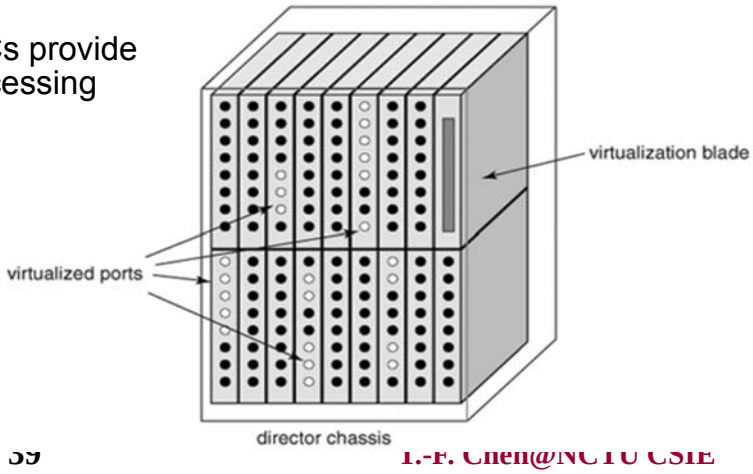


Network-based Virtualization

- Requirements of storage network
  - Intelligent services
    - Logon services
    - Simple name server
    - Change notification
    - Network address assignment
    - Zoning
  - Fabric switch should provide
    - Connectivity for all storage transactions
    - Interoperability between disparate servers, operating systems, and target devices

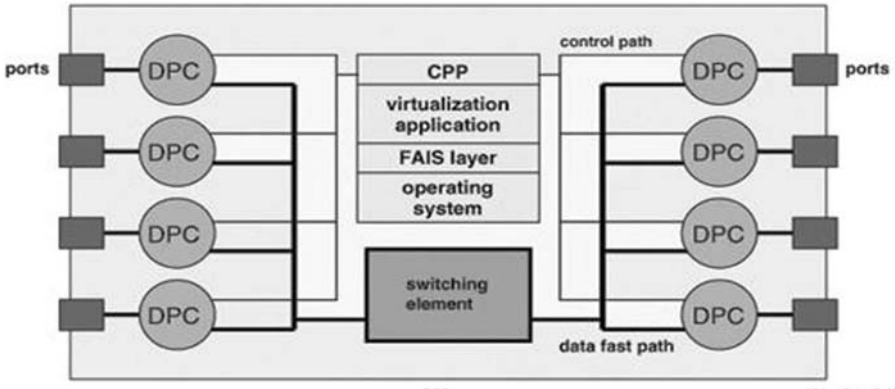
Network-based Virtualization

- Techniques for fabric switch virtualization
  - Hosted on departmental switches
    - A PC engine provisioned as an option blade.
  - Data center directors
    - Should be able to preserve the five nines availability characteristic of director-class switches.
    - Dedicated virtualization ASICs provide high-performance frame processing and block address mapping.
  - Interoperability between different implementations will become a priority.



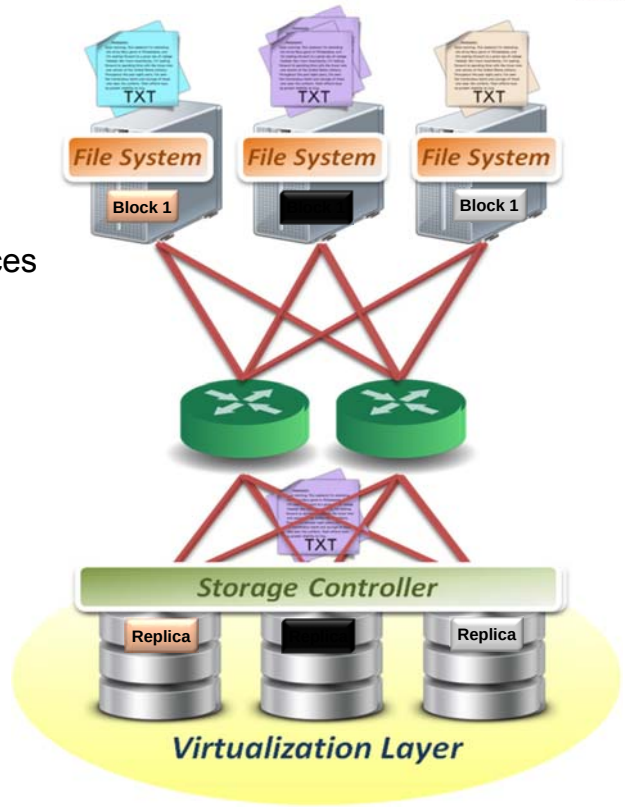
Network-based Virtualization

- Interoperability issue
  - FAIS (*Fabric Application Interface Standard*)
    - Define a set of standard APIs to integrate applications and switches.
    - FAIS separates control information and data paths.
    - The control path processor (CPP) supports the FAIS APIs and upper layer storage virtualization application.
    - The data path controller (DPC) executes the virtualized SCSI I/Os under the management of one or more CPPs



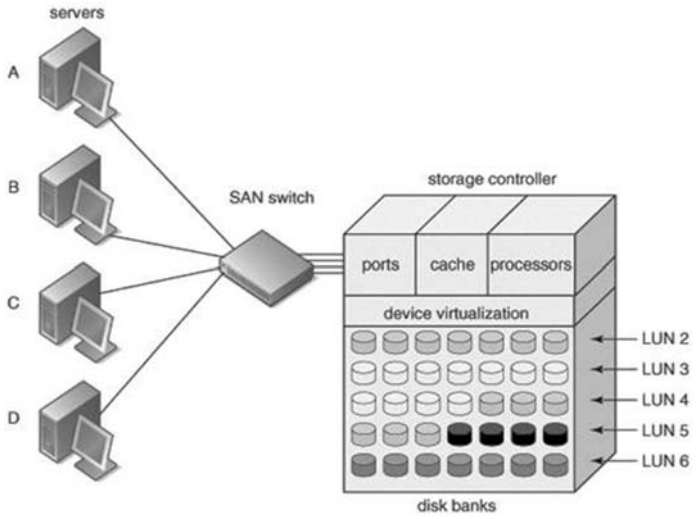
Storage-based Virtualization

- Storage-based approach
  - File level
    - Run software on storage device to provide file based data storage services to host through network.
  - Block level
    - Embeds the technology in the target storage devices.
  - Provide services
    - Storage pooling
    - Replication and RAID
    - Data sharing and tiering



Storage-based Virtualization

- Array-based virtualization
  - Storage controller
    - Provide basic disk virtualization in the form of RAID management, mirroring, and LUN mapping or masking.
    - Allocate a single LUN to multiple servers.
    - Offer Fibre Channel, iSCSI, and SCSI protocol.
  - Cache memory
    - Enhance performance.
  - Storage assets coordination
    - Coordination between multiple storage systems is necessary to ensure high availability.



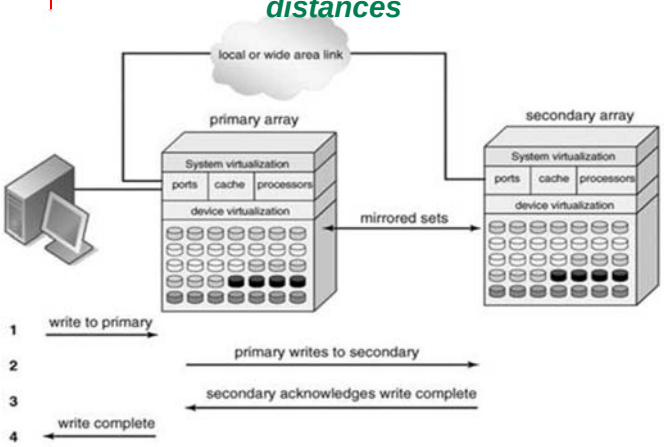
Storage-based Virtualization

- Data replication
  - Array-based data replication
    - Referred to as disk-to-disk replication.
    - Requires that a storage controller function concurrently as both an initiator and target.
  - Synchronous vs. Asynchronous
    - Synchronous data replication ensures that a write operation to a secondary disk array is completed before the primary array acknowledges task completion to the server.
    - Asynchronous data replication provides write completion by the primary array, although the transaction may still be pending to the secondary array.

Storage-based Virtualization

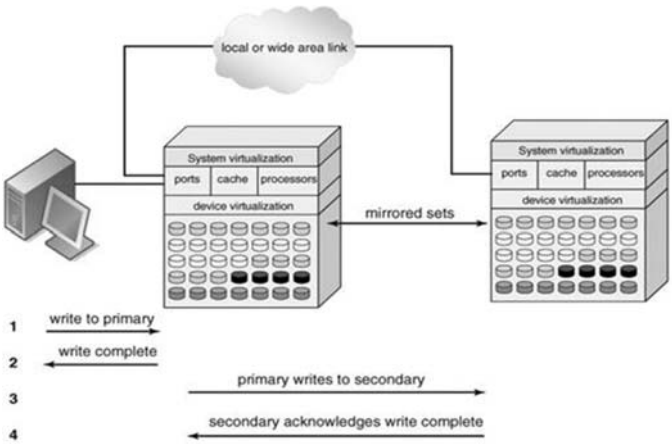
Synchronous

To preserve performance, synchronous data replication is limited to metropolitan distances



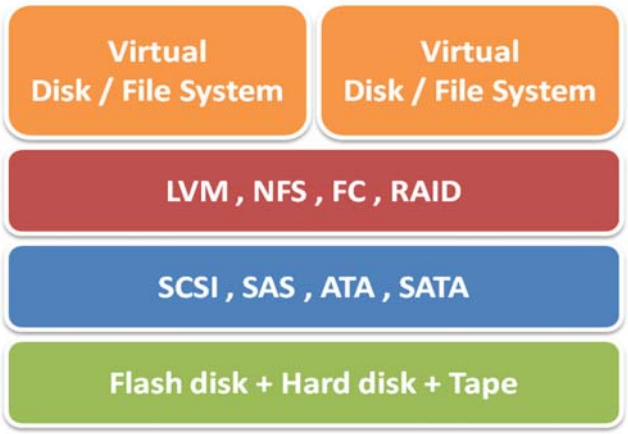
Asynchronous

Asynchronous data replication is largely immune to transmission latency



Summary

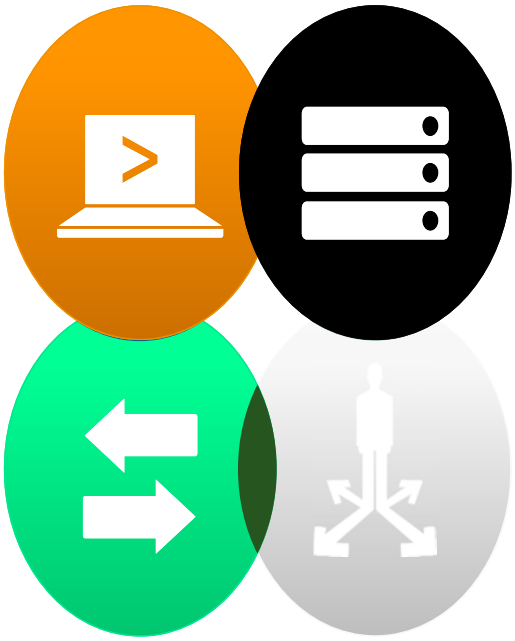
- Storage virtualization technique :
  - Virtualization layer
    - File level and block level
  - Virtualization location
    - Host, network and storage base
  - Virtualization method
    - In-band and out-of-band
- Storage virtualization services
  - Storage pooling and sharing
  - Data replication and mirroring
  - Snapshot and multi-pathing



The Software-Defined Data Center

Expand virtual compute to all applications

Virtualize the network for speed and efficiency

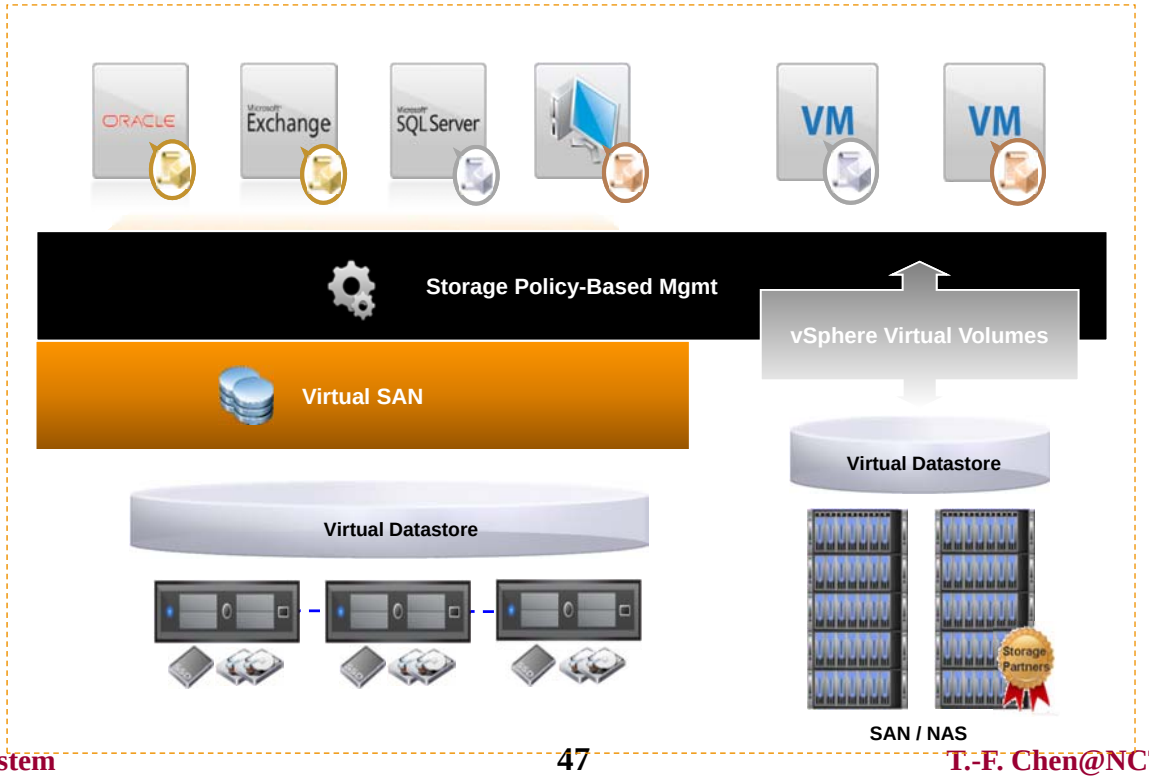


Transform storage by aligning it with app demands

Management tools give way to automation

VMware Software-Defined Storage

Bringing the Efficient Operational Model of Virtualization to Storage and Availability



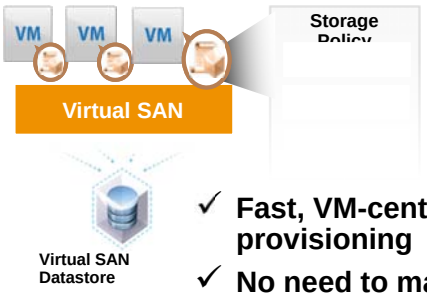
Virtual SAN Puts The App In Charge

VM-centric Service Levels for Simpler and Automated Storage Management Through App-centric Approach

Today

- ✖ Hardware-centric, vendor-specific management
- ✖ Slow provisioning, rigid storage constructs (LUNs, Volumes)
- ✖ Data services aligned to storage container, not directly with VM needs
- ✖ Frequent data migrations

Virtual SAN

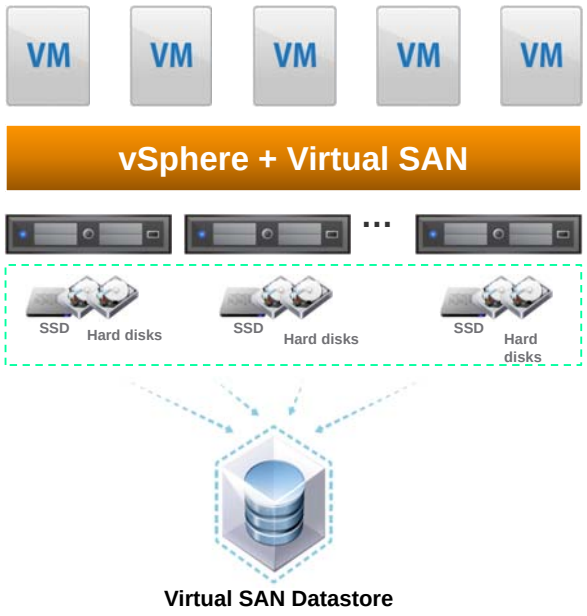


- ✓ Fast, VM-centric provisioning
- ✓ No need to manage LUNs, Vols.
- ✓ Resources and data service are automatically provisioned and maintained
- ✓ Easy to change without data migration

48

VMware Virtual SAN : Hybrid

Radically Simple Hypervisor-Converged Storage Software

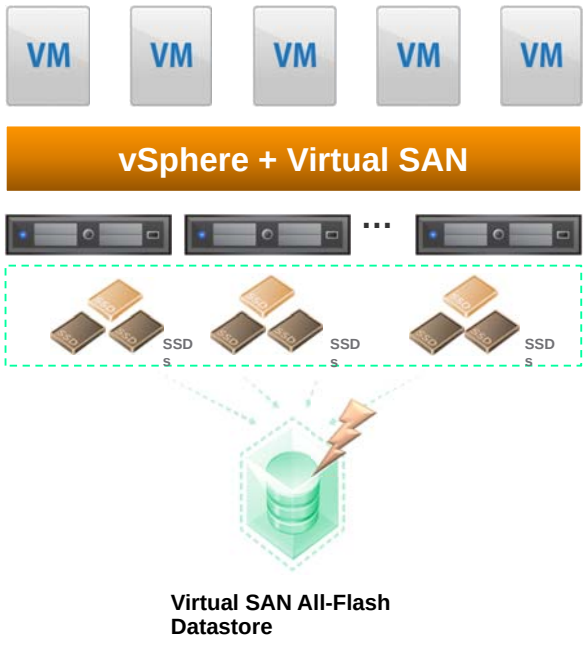


Virtual SAN

- Software-defined storage built into vSphere
- Runs on any standard x86 server
- Pools flash-based devices into a shared datastore
- Managed through per-VM storage policies
- Delivers High performance through flash acceleration
- 2x more IOPS with VSAN Hybrid
  - Up to 40K IOPS/host
- Highly resilient - zero data loss in the event of hardware failures
- Deeply integrated with the VMware stack

VMware Virtual SAN : All-Flash

Extremely High Performance with Predictability



Virtual SAN All-Flash

- Flash-based devices used for caching as well as persistence
- Cost-effective all-flash 2-tier model:
  - Cache is 100% write: using write-intensive, higher grade flash-based devices
  - Persistent storage: can leverage lower cost read-intensive flash-based devices
- Very high IOPS: up to 90K(1) IOPS/Host
- Consistent performance with sub-millisecond latencies

Enterprise-Class Scale and Performance

	Virtual SAN 5.5	Virtual SAN 6.0 Hybrid	Virtual SAN 6.0 All-Flash
Hosts / Cluster	32	64	64
IOPS / Host	20K	40K	90K
VMs / Host	100	200	200
VMs / Cluster	3200	6400	6400

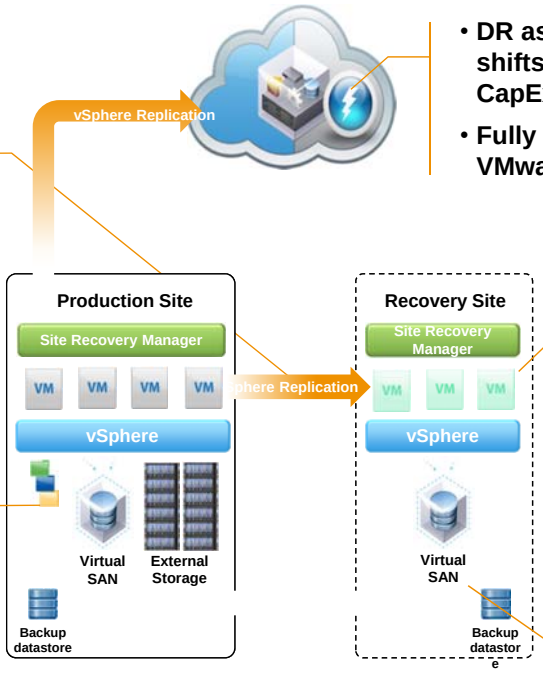
Disaster Recovery For The Software-Defined Data Center

vSphere Replication

- VM-centric, storage-independent replication simplifies protection
- Flexible storage topologies (External to Virtual SAN or vCloud Air)

vSphere Data Protection Advanced

- Storage-efficient dedupe reduces storage investments
- WAN-efficient backup data replication enables basic DR



vCloud Air Disaster Recovery

- DR as a Service to vCloud Air shifts DR investments from CapEx to OpEx
- Fully delivered and supported by VMware

Site Recovery Manager

- Centralized recovery plans enables DR scale for thousands of VMs
- DR workflow automation reduces OpEx on DR management

Virtual SAN

- Server side economics lower storage costs
- Hyper-convergence on x86 platform reduces DR footprint