



# INFORMATION STORAGE AND MANAGEMENT V5

**PARTICIPANT GUIDE**





# Table of Contents

Information Storage and Management v5 .....	21
<b>Introduction to Information Storage .....</b>	<b>22</b>
<b>Introduction to Information Storage .....</b>	<b>23</b>
Data Storage: Ever Changing and Ever Growing.....	24
Why Information Storage and Management.....	25
Data and Information.....	26
Information Storage.....	28
Data Center.....	29
Key Characteristics of a Modern Data Center.....	30
Digital Transformation .....	32
Business Drivers of Digital Transformation .....	33
<b>Knowledge Check.....</b>	<b>34</b>
Knowledge Check .....	35
Knowledge Check .....	36
<b>Business Drivers of Digital Transformation .....</b>	<b>37</b>
Business Drivers of Digital Transformation .....	38
<b>Cloud Computing .....</b>	<b>39</b>
Cloud Computing.....	40
Cloud Computing Overview .....	41
Cloud Computing Characteristics.....	42
Cloud Computing Benefits.....	45
Cloud Service Models .....	47
Cloud Deployment Models .....	49
Cloud Computing: Use Cases.....	51
<b>Knowledge Check.....</b>	<b>53</b>
Knowledge Check .....	54

<b>Big data .....</b>	<b>55</b>
Big Data .....	56
Big Data Overview.....	57
Characteristics of Big Data .....	58
Big Data Analytics .....	60
Big Data: Use Cases .....	61
<b>Knowledge Check.....</b>	<b>63</b>
Knowledge Check .....	64
<b>Artificial Intelligence and Machine Learning.....</b>	<b>65</b>
Artificial Intelligence and Machine Learning .....	66
AI/ML Overview.....	67
AI/ML Machine Learning Methods .....	69
<b>Knowledge Check.....</b>	<b>70</b>
Knowledge Check .....	71
<b>Internet of Things (IoT) .....</b>	<b>72</b>
Internet of Things (IoT) .....	73
Internet of Things (IoT) Overview .....	74
IoT Architecture.....	75
Internet of Things: Use Cases .....	77
<b>Knowledge Check.....</b>	<b>79</b>
Knowledge Check .....	80
<b>Edge Computing.....</b>	<b>81</b>
Edge Computing .....	82
Edge Computing Overview .....	83
Edge Computing: Use Cases .....	84
<b>Knowledge Check.....</b>	<b>87</b>
Knowledge Check .....	88
<b>5G .....</b>	<b>89</b>
5G Overview .....	90
Information Storage and Management v5	

5G Features .....	91
5G: Case Study.....	92
<b>Knowledge Check.....</b>	<b>94</b>
Knowledge Check .....	95
<b>Concepts in Practice.....</b>	<b>96</b>
Concepts in Practice .....	97
<b>Modern Data Center Environment.....</b>	<b>99</b>
Modern Data Center Environment .....	100
<b>Compute Systems .....</b>	<b>101</b>
Compute Systems .....	102
Types of Compute Systems .....	103
Compute Virtualization .....	104
Hypervisor .....	105
Virtual Machine .....	106
Containers.....	108
Containers vs. VMs .....	109
Desktop Virtualization.....	110
Virtual Machine and Container Lab Demo .....	112
<b>Knowledge Check.....</b>	<b>113</b>
Knowledge Check .....	114
<b>Applications.....</b>	<b>115</b>
Applications.....	116
Traditional Applications .....	117
Cloud-Native Applications.....	118
Application Virtualization.....	119
<b>Knowledge Check.....</b>	<b>121</b>
Knowledge Check .....	122
<b>Storage.....</b>	<b>123</b>
Information Storage and Management v5	

Storage .....	124
Types of Storage.....	125
Storage Architecture: DAS vs. SAN.....	127
Storage Virtualization .....	129
<b>Knowledge Check.....</b>	<b>130</b>
Knowledge Check .....	131
<b>Network.....</b>	<b>132</b>
Network.....	133
Network Overview .....	134
Network Communication Protocols.....	139
The OSI Reference Model.....	140
TCP/IP Reference Model.....	141
IP Addressing.....	142
Network Virtualization .....	143
<b>Knowledge Check.....</b>	<b>144</b>
Knowledge Check .....	145
Knowledge Check .....	146
<b>Software-Defined Data Center (SDDC) .....</b>	<b>147</b>
Software-Defined Data Center (SDDC) .....	148
Software-Defined Data Center (SDDC) Overview.....	149
Software-Defined Data Center Architecture .....	150
<b>Knowledge Check.....</b>	<b>152</b>
<b>Modern Data Center Architecture.....</b>	<b>154</b>
Modern Data Center Architecture .....	155
Modern Data Center Architecture .....	156
<b>Knowledge Check.....</b>	<b>158</b>
Knowledge Check .....	159
<b>Building a Modern Data Center .....</b>	<b>160</b>

Do-It-Yourself Approach .....	161
DIY Methods .....	162
Vendor Ready Solutions .....	163
Converged and Hyper-Converged Infrastructure.....	164
Data Center as a Service (DCaaS).....	166
<b>Knowledge Check.....</b>	<b>167</b>
Knowledge Check .....	168
<b>Concepts in Practice.....</b>	<b>169</b>
Concepts in Practice .....	170
<b>Intelligent Storage System .....</b>	<b>174</b>
Intelligent Storage Systems .....	175
<b>Intelligent Storage System (ISS) Overview .....</b>	<b>176</b>
Intelligent Storage System (ISS) Overview .....	177
Key Features of an Intelligent Storage System .....	178
Intelligent Storage System Types .....	180
ISS Types: Additional Information.....	184
<b>Knowledge Check.....</b>	<b>185</b>
Knowledge Check .....	186
<b>Intelligent Storage System Components.....</b>	<b>187</b>
Intelligent Storage System Components.....	188
Intelligent Storage System Components.....	189
Hard Disk Drive .....	191
Hard Disk Drive Performance .....	193
Why Flash Storage? .....	195
Solid State Drive.....	200
Solid State Drive Performance.....	202
Non-Volatile Memory Express (NVMe) .....	203
Storage Class Memory.....	204
<b>RAID .....</b>	<b>206</b>

RAID Overview.....	207
RAID Techniques .....	208
RAID Levels .....	210
RAID 1+0 .....	211
RAID 5 .....	212
RAID 6 .....	213
RAID Impacts on Performance .....	214
RAID Concepts: Additional Information.....	216
<b>Knowledge Check.....</b>	<b>217</b>
Knowledge Check .....	218
<b>Storage Provisioning .....</b>	<b>219</b>
Storage Provisioning Overview.....	220
Traditional Provisioning .....	221
Virtual Provisioning.....	222
Traditional Provisioning vs. Virtual Provisioning .....	224
<b>Storage Tiering .....</b>	<b>226</b>
Storage Tiering Overview .....	227
Tiering Within a Storage System .....	229
Tiering Between Storage Systems.....	230
Cache Tiering.....	231
<b>Knowledge Check.....</b>	<b>233</b>
Knowledge Check .....	234
<b>Block, File and Object-based Storage Systems .....</b>	<b>235</b>
Block, File and Object-Based Storage Systems.....	236
<b>Block-Based Storage Systems .....</b>	<b>237</b>
Block, File, and Object-Based Storage Systems.....	238
Block-Based Storage Systems .....	239
Block-Based Storage System Overview .....	240
Block Storage System Components .....	241

Cache Operations .....	245
Block Storage System Disk Drive Protocols.....	247
Use Case - Block-Based Storage in the Cloud.....	249
<b>Knowledge Check.....</b>	<b>251</b>
Knowledge Check .....	252
<b>File-Based Storage Systems .....</b>	<b>254</b>
File-Based Storage System (NAS).....	255
File Systems and Network File Sharing .....	256
File-Based Storage Systems: Network Attached Storage (NAS) .....	259
General Purpose Servers Vs. NAS Systems .....	260
NAS Components.....	261
Scale-Up NAS .....	263
Scale-Out NAS.....	264
Network File Sharing Access Protocols .....	266
NAS I/O Operation .....	270
Use-Case for Scale-Out NAS: Data Lake .....	273
<b>Knowledge Check.....</b>	<b>275</b>
Knowledge Check .....	276
<b>Object-Based Storage Systems.....</b>	<b>277</b>
Drivers for Object-Based Storage .....	278
What is an Object in Object-Based Storage?.....	280
Hierarchical File System Vs. Flat Address Space .....	281
Components of Object-Based Storage Device.....	282
Key Features of OSD Storage Systems.....	284
Use Case: Cloud-Based Storage.....	287
Use Case: Cloud-based Object Storage Gateway .....	288
<b>Knowledge Check.....</b>	<b>290</b>
Knowledge Check .....	291
Knowledge Check .....	292
<b>Unified Storage Systems .....</b>	<b>293</b>
Unified Storage Systems .....	294
Information Storage and Management v5	

Drivers for Unified Storage Systems .....	295
Unified Storage System Architecture .....	296
<b>Concepts in Practice.....</b>	<b>297</b>
Concepts in Practice .....	298
<b>Storage Area Networking - FC SAN .....</b>	<b>302</b>
Storage Area Network - FC SAN .....	303
<b>Introduction to SAN .....</b>	<b>304</b>
Business Needs and Technology Challenges .....	305
SAN Overview.....	306
<b>Knowledge Check.....</b>	<b>307</b>
Knowledge Check .....	308
<b>Fibre Channel SAN.....</b>	<b>309</b>
FC SAN Overview .....	310
FC SAN Components.....	311
FC Network Interconnecting Devices.....	314
FC SAN Device Port Types .....	315
FC SAN Protocol Stack .....	316
FC Frame.....	318
FC Addressing in Switched Fabric.....	319
World Wide Name .....	320
FC SAN: Additional Information .....	321
<b>Knowledge Check.....</b>	<b>322</b>
Knowledge Check .....	323
<b>FC SAN Topologies, Link Aggregation and Zoning.....</b>	<b>324</b>
FC SAN Topologies, Link Aggregation and Zoning .....	325
FC SAN Topologies.....	326
Link Aggregation .....	329
FC SAN Zoning .....	331
FC SAN Zoning Types .....	333

FC Fabric: Additional Information .....	336
<b>Knowledge Check.....</b>	<b>337</b>
Knowledge Check .....	338
<b>SAN Virtualization .....</b>	<b>339</b>
Block-level Storage Virtualization.....	340
Virtual Fabric - VSAN .....	342
<b>Knowledge Check.....</b>	<b>343</b>
Knowledge Check .....	344
<b>Concepts in Practice.....</b>	<b>345</b>
Concepts in Practice .....	346
<b>Exercise .....</b>	<b>349</b>
Exercise: FC SAN Topologies .....	350
<b>IP SAN, FCoE and NVMe-oF .....</b>	<b>352</b>
IP SAN, FCoE and NVMe-oF .....	353
<b>Overview of IP SAN .....</b>	<b>354</b>
Module Objectives .....	355
Overview of IP SAN.....	356
IP SAN Overview .....	357
IP SAN Protocols .....	358
<b>iSCSI.....</b>	<b>361</b>
iSCSI Overview .....	362
iSCSI Components.....	363
Native and Bridged iSCSI Connectivity .....	365
iSCSI Protocol Stack.....	368
iSCSI Addressing and Naming .....	370
Virtual LAN (VLAN) .....	372
VLAN Tagging.....	374
iSCSI: Additional Information .....	375

<b>Knowledge Check.....</b>	<b>376</b>
Knowledge Check .....	377
Knowledge Check .....	378
<b>FCIP .....</b>	<b>379</b>
FCIP Overview .....	380
Fibre Channel Over IP (FCIP) .....	381
FCIP Connectivity.....	382
FCIP Protocol Stack and Frame Encapsulation .....	383
FCIP Connectivity: Additional Information.....	386
<b>Knowledge Check.....</b>	<b>387</b>
Knowledge Check .....	388
<b>FCoE.....</b>	<b>389</b>
FCoE Overview .....	390
Fibre Channel Over Ethernet (FCoE).....	391
FC Frame Encapsulation .....	393
FCoE: Additional Information.....	394
<b>NVMe Over Fabrics.....</b>	<b>395</b>
NVMe Over Fabrics Overview .....	396
NVM Express Overview.....	397
NVMe Over Fabrics.....	399
NVMe Over Fibre Channel (FC-NVMe) .....	401
NVMe Over Fabrics Device Addressing.....	403
<b>Knowledge Check.....</b>	<b>404</b>
Knowledge Check .....	405
<b>Concepts in Practice.....</b>	<b>406</b>
Concepts in Practice .....	407
<b>Software Defined Storage and Network.....</b>	<b>412</b>
Software Defined Storage and Network .....	413
<b>Software-Defined Storage.....</b>	<b>414</b>

Need for Software-Defined Storage.....	415
Software-Defined Storage (SDS).....	416
Key Attributes of Software-Defined Storage.....	417
Software-Defined Storage Architecture.....	419
Benefits of Software-Defined Storage.....	422
<b>Knowledge Check.....</b>	<b>423</b>
Knowledge Check .....	424
<b>Software-Defined Networking (SDN).....</b>	<b>425</b>
Software-Defined Networking .....	426
Introduction to Software-Defined Networking.....	427
Software-Defined Networking Benefits .....	428
Software-Defined Networking Architecture.....	430
Software-Defined Networking Use Case.....	432
<b>Knowledge Check.....</b>	<b>435</b>
Knowledge Check .....	436
<b>Concepts in Practice.....</b>	<b>437</b>
Concepts in Practice .....	438
<b>Business Continuity.....</b>	<b>440</b>
Business Continuity.....	441
<b>Business Continuity Overview.....</b>	<b>442</b>
Business Continuity .....	443
Information Availability.....	445
Causes of Information Unavailability .....	447
Impact of Information Unavailability .....	449
Measurement of Information Availability .....	450
RPO and RTO.....	452
Disaster Recovery .....	454
Business Continuity Technology Solutions .....	455
<b>Knowledge Check.....</b>	<b>457</b>

Knowledge Check .....	458
<b>Fault Tolerance Infrastructure.....</b>	<b>459</b>
Fault Tolerance Infrastructure.....	460
Fault Tolerance IT Infrastructure Overview .....	461
Key Requirements for Fault Tolerance .....	462
Fault Isolation.....	463
Single Points of Failure.....	464
Eliminating Single Points of Failure .....	465
Eliminating Single Points of Failure: Additional Information.....	466
Compute Clustering.....	467
Network Fault Tolerance Mechanisms.....	468
Storage Fault Tolerance Mechanisms .....	471
Fault Tolerance at Site-Level – Availability Zones.....	474
<b>Knowledge Check .....</b>	<b>475</b>
Knowledge Check .....	476
<b>Concepts in Practice.....</b>	<b>477</b>
Concepts in Practice .....	478
<b>Exercise - Business Continuity.....</b>	<b>479</b>
Exercise: Information Availability .....	480
Exercise: MTBF and MTTR .....	482
<b>Data Protection.....</b>	<b>484</b>
Data Protection .....	485
<b>Data Replication .....</b>	<b>486</b>
Data Replication Overview .....	487
Use of Replicas .....	489
Data Replication: Additional Information .....	491
Types of Replication.....	492
Local Replication: Snapshot .....	493
Local Replication: Clone .....	495
Remote Replication: Synchronous.....	496

Remote Replication: Asynchronous .....	498
Replication Types: Additional Information .....	500
Continuous Data Protection (CDP) .....	501
Key Continuous Data Protection Components .....	503
Continuous Data Protection: Local and Remote Replication .....	504
CDP: Additional Information .....	505
 Knowledge Check .....	507
<b>Data Backup.....</b>	<b>508</b>
Data Backup .....	509
Backup Overview .....	510
Backup Architecture .....	511
Backup Operation.....	512
Recovery Operation .....	513
Backup Granularities .....	514
Agent-Based Backup.....	519
Image-Based Backup .....	520
Cloud-Based Backup (Backup as a Service) .....	522
Backup Architecture: Additional Information.....	523
Backup and Recovery Lab Demo .....	524
 Knowledge Check.....	525
Knowledge Check .....	526
<b>Data Deduplication .....</b>	<b>527</b>
Data Deduplication Overview .....	528
Key Benefits of Data Deduplication .....	531
Data Deduplication Method: Source-Based .....	532
Data Deduplication Method: Target-Based .....	533
Data Deduplication: Additional Information .....	534
 Knowledge Check.....	535
Knowledge Check .....	536
<b>Data Archiving.....</b>	<b>537</b>
Data Archiving Overview .....	538

Backup vs. Archive.....	539
Data Archiving Operations.....	540
Use Case: Email Archiving .....	541
<b>Knowledge Check.....</b>	<b>543</b>
Knowledge Check .....	544
<b>Data Migration .....</b>	<b>545</b>
Data Migration Overview .....	546
Hypervisor-Based Migration .....	547
Storage-Based Data Migration.....	549
Appliance-Based Data Migration .....	551
VM Migration: Additional Information .....	552
<b>Knowledge Check.....</b>	<b>553</b>
Knowledge Check .....	554
<b>Concepts in Practice.....</b>	<b>555</b>
Concepts in Practice .....	556
<b>Exercise: Data Protection .....</b>	<b>562</b>
Exercise: Data Protection .....	563
<b>Storage Infrastructure Security.....</b>	<b>566</b>
Storage Infrastructure Security .....	567
<b>Introduction to Information Security .....</b>	<b>568</b>
Introduction to Information Security .....	569
Information Security: Key Terminologies.....	570
Governance, Risk and Compliance (GRC) .....	571
Authentication, Authorization, and Auditing.....	573
Security Concepts .....	575
Storage Security Domains.....	577
<b>Knowledge Check.....</b>	<b>579</b>
Knowledge Check .....	580

Key Security Threats .....	582
<b>Knowledge Check.....</b>	<b>586</b>
Knowledge Check .....	587
<b>Security Controls .....</b>	<b>588</b>
Defense-in-depth.....	589
Security Controls.....	590
Identity and Access Management (IAM) .....	594
Multifactor Authentication .....	595
OAuth and OpenID.....	596
Role-Based Access Control.....	600
Malware Protection Software.....	602
Mobile Device Management .....	604
Data Encryption.....	606
Data Shredding .....	608
Cyber Recovery .....	609
Penetration Testing .....	611
VM, OS and Application Hardening .....	612
<b>Knowledge Check.....</b>	<b>615</b>
Knowledge Check .....	616
Knowledge Check .....	617
<b>Concepts in Practice.....</b>	<b>618</b>
Concepts in Practice .....	619
<b>Exercise - Storage Infrastructure Security.....</b>	<b>621</b>
Exercise: Storage Infrastructure Security.....	622
<b>Storage Infrastructure Management .....</b>	<b>624</b>
Storage Infrastructure Management .....	625
<b>Storage Infrastructure Management.....</b>	<b>626</b>
Overview .....	627
Key Characteristics of Modern Storage Infrastructure Management .....	628
Key Storage Management Functions .....	630

<b>Operations Management.....</b>	<b>631</b>
Monitoring .....	632
Monitoring Parameters .....	633
Alerts.....	641
Reporting .....	642
Operations Management Processes.....	644
<b>Knowledge Check.....</b>	<b>653</b>
Knowledge Check .....	654
Knowledge Check .....	655
Knowledge Check .....	656
<b>Concepts in Practice.....</b>	<b>657</b>
Concepts in Practice .....	658
<b>Exercise - Storage Infrastructure Management .....</b>	<b>663</b>
Exercise: Storage Infrastructure Management .....	664
<b>Summary .....</b>	<b>666</b>
Summary.....	667
<b>Course Assessment.....</b>	<b>668</b>
<b>Assessment Questions.....</b>	<b>669</b>
Question.....	670
Question.....	671
Question.....	672
Question.....	673
Question.....	674
Question.....	675
Question.....	676
Question.....	677
Question.....	678
Question.....	679
Question.....	680

Question.....	681
Question.....	682
Question.....	683
Question.....	684
<b>Course Completion .....</b>	<b>685</b>



## Introduction to Information Storage

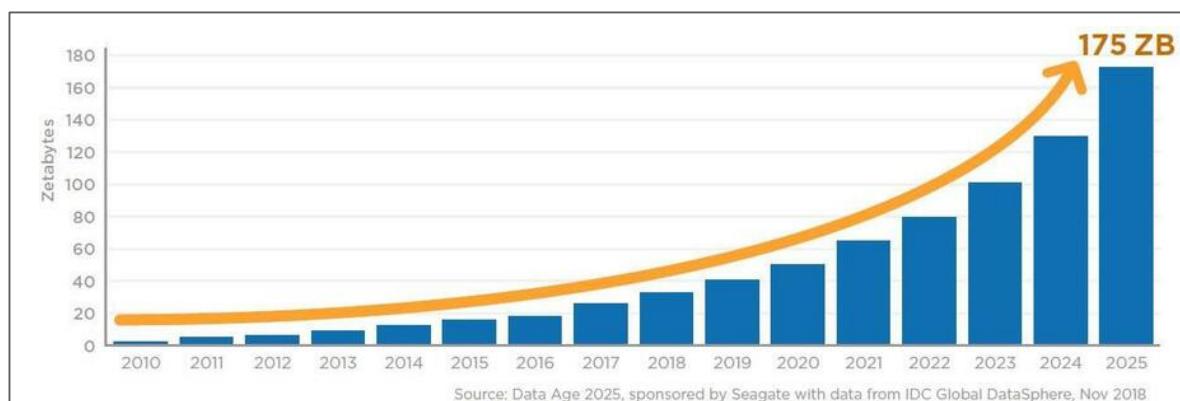
## Information Storage and Management v5

# Introduction to Information Storage

## Introduction to Information Storage

## Data Storage: Ever Changing and Ever Growing

- Digital universe is created and defined by software.
  - Digital data is continuously generated, collected, stored, and analyzed through software.
- IDC report predicts worldwide data creation grows to an enormous 175 zettabytes (ZB) by 2025.
- Technologies driving digital transformation add to data growth.



*Data growth prediction by IDC (Click image to enlarge)*

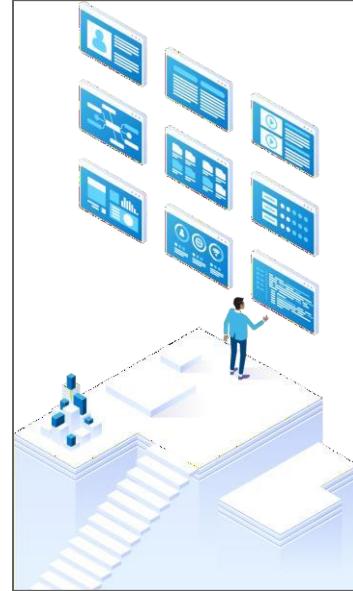
### Notes:

We live in a digital universe where a massive amount of digital data is continuously generated, collected, stored, and analyzed through software.

The data in the digital universe comes from diverse sources, including both individuals and organizations. Individuals constantly generate and consume information through numerous activities, such as web searches, email messages, uploading and downloading content and sharing media files. In organizations, the volume and importance of information for business operations continue to grow at astounding rates. Technologies driving digital transformation including Internet of Things (IoT) have contributed to the growth of the digital data.

## Why Information Storage and Management

- Organizations have become increasingly information-dependent in the 21st century, and information must be available whenever and wherever it is required.
- Organizations seek to store, protect, process, manage, and use information.
- Businesses can leverage this data to:
  - Identify new customers.
  - Retain existing customers.
  - Predict sales volumes.
  - Improve customer service.



### Notes:

It is critical for users and applications to have continuous, fast, reliable, and secure access to information for business operations to run as required.

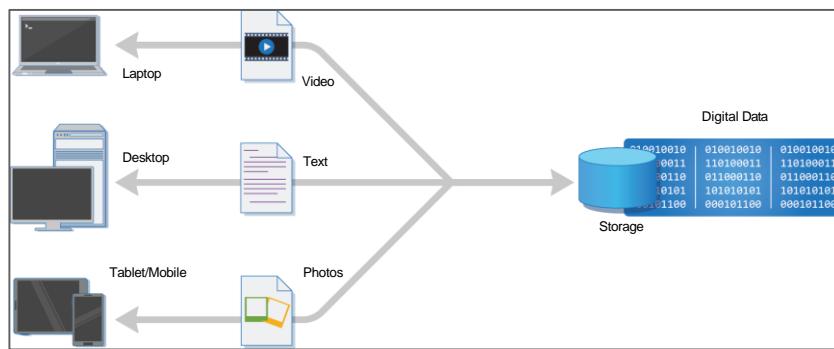
Data is the lifeblood of a rapidly growing digital existence, opening new opportunities for businesses, and gain a competitive edge.

Overall, data helps business leaders make smarter decisions about where to take their companies.

It is essential for organizations to store, protect, process, and manage information in an efficient and cost-effective manner. Legal, regulatory, and contractual obligations regarding the availability, retention, and protection of data further add to the challenges of storing and managing information.

To meet all these requirements, organizations are increasingly undertaking digital transformation initiatives and implement intelligent storage solutions. These solutions enable efficient and optimized storage and management of information. The solutions also enable extraction of value from information to derive new business opportunities, gain a competitive advantage, and create sources of revenue.

### Data and Information



*Storing digital data (Click image to enlarge)*

**Digital data** is transmitted and stored in electronic form, and processed through software.

- Devices such as desktops, laptops, tablets, mobile phones, and electronic sensors generate digital data.
- Two types of data are structured<sup>1</sup> and unstructured<sup>2</sup> data.
- Information is processed data that enables useful interpretation and decision-making.

---

<sup>1</sup> Structured data is organized in fixed fields within a record or file. To structure the data, you require a data model. A data model specifies the format for organizing data, and also specifies how different data elements are related to each other. For example, in a relational database, data is organized in rows and columns within named tables.

<sup>2</sup> Unstructured data does not have a data model and is not organized in any particular format. Some examples of unstructured data include text documents, PDF files, email messages, presentations, images, and videos.

- Example: Annual sales data processed into a sales report

### Notes:

A generic definition of data is that it is a collection of facts, typically collected for analysis or reference. Data can exist in various forms such as facts stored in a person's mind, photographs, a bank ledger, and tabled results of a scientific survey.

Devices such as desktops, laptops, tablets, mobile phones, and electronic sensors generate digital data. Digital data is stored as strings of binary values on a storage medium. Examples of digital data are electronic documents, text files, email messages, ebooks, digital images, digital audio, and digital video.

Information is processed data to enable useful interpretation and decision-making. For example, when you process the annual sales data into a sales report, it provides useful information. The information can be the average sales for a product (indicating product demand and popularity), and a comparison of the actual sales to the projected sales.

## Information Storage



*Different storage devices*

- Information is stored on a choice of non-volatile media such as:
  - Magnetic storage devices (Hard disk drive and magnetic tape drive).
  - Optical storage devices (Blu-ray, DVD, and CD).
  - Flash-based storage devices: Solid-state drive (SSD), memory card, and USB thumb drive.
- Storage devices are assembled within a storage system or “array”.
  - Storage systems provide high capacity, scalability, performance, availability, reliability, and security.
- Storage systems along with other IT infrastructure are housed in a data center.

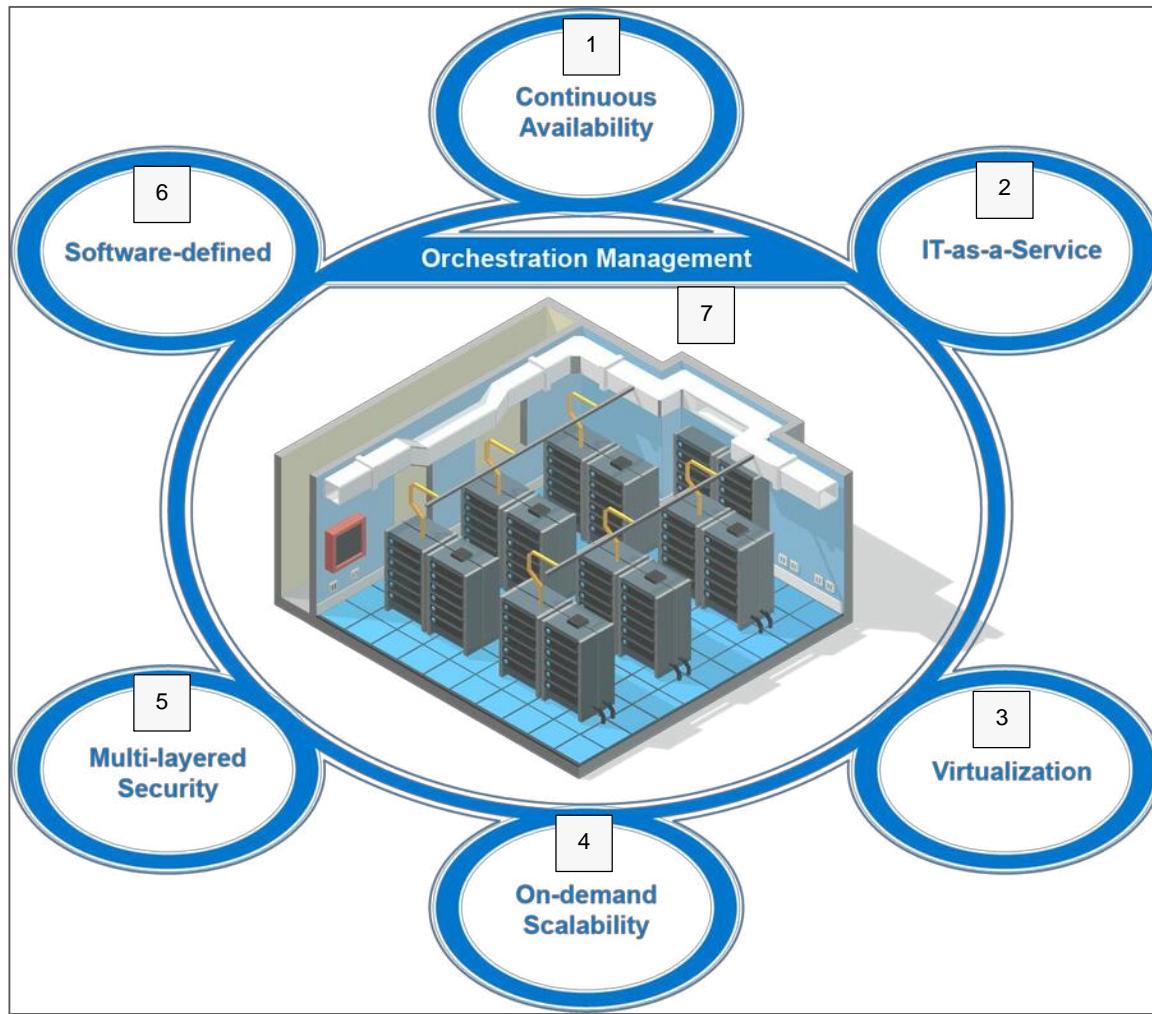
## Data Center



- A data center typically consists of:
  - **Facility:** The building and floor space where the data center is constructed.
  - **IT equipment:** Compute system, storage, and network components.
  - **Support infrastructure:** Power supply, fire detection, HVAC, and security systems
- A data center may be constructed in-house (located in an organization's own facility).
  - The data center may also be outsourced, with equipment being at a third-party site.

## Key Characteristics of a Modern Data Center

Data centers are designed and built to fulfill the key characteristics as shown in the figure.



**1:** A data center should ensure 24x7x365 availability of resources to provide anytime, anywhere data access.

**2:** A data center should adopt the IT resource delivery as a service paradigm. It enables the IT department of an organization to become a utility to the business. Also, delivers IT resources as services for convenient consumption by business units. IT services are maintained in a service catalog which enables users to provision resources in a self-service manner.

- 3:** It is the process of abstracting physical resources, such as compute, storage, and network, and creating virtual resources from them. A virtualized data center provides the flexibility to create and reclaim virtual resources dynamically.
- 4:** The data center IT infrastructure should be designed for scalable computing. It enables the IT resources to scale-up, and down quickly as the demand for resources grows and shrinks.
- 5:** Multiple layers of security help in mitigating the risk of security threats in case one layer is compromised. An attacker must breach each layer to be successful. This approach provides additional time to detect and respond to an attack.
- 6:** A software-defined data center supports software-centric control of data center resources. A controller software that is decoupled from hardware sends instructions to the hardware components to perform the required operations.
- 7:** Orchestration of management operations helps in improving business agility. Orchestration enables automated arrangement and coordination of various component functions that is based on a predefined workflow.

## Digital Transformation



*To view the video about digital transformation imperatives, click [here](#).*

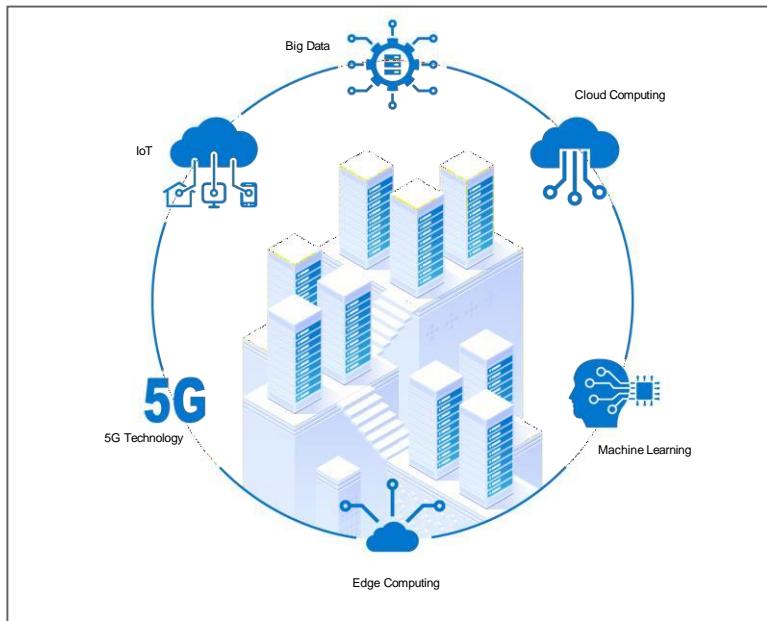
Today, people live in a digital world, and organizations must deliver exceptional customer experiences with their products and services to meet their customers' expectations.

To meet the needs of the customers and be competitive in the market place, organizations have to adopt digital transformation.

Digital Transformation can be achieved using smarter products, data analytics, and continuous improvement of products and services using software. For businesses, it is now critical to digitally transform to meet the demands of their customers.

## Business Drivers of Digital Transformation

- In this digital world, organizations must develop new applications using agile processes and new tools to achieve rapid time-to-market. Simultaneously, the organizations still expect IT to operate and manage the traditional applications that provide revenue.



*Key technologies to enable digital transformation*

- Organizations are also under pressure to manage the enormous growth of digital data and derive new values from the data. To survive, the organization must transform and adopt modern technologies to support the digital transformation.
- Some of the key technologies that enable digital transformation are:
  - Cloud Computing
  - Big Data
  - Artificial Intelligence and Machine Learning
  - Internet of Things (IoT)
  - Edge Computing
  - 5G

Knowledge Check

## Knowledge Check

## Knowledge Check

1. Which modern data center characteristic helps in improving business agility by automated arrangement and coordination of various component functions that is based on a predefined workflow?
  - a. Continuous availability
  - b. On-demand scalability
  - c. Orchestrated management
  - d. Virtualization

## Knowledge Check

### Knowledge Check

2. Why are businesses undergoing digital transformation?
  - a. To eliminate security threats
  - b. To meet regulatory requirements
  - c. To innovate more quickly
  - d. To eliminate management costs

## Business Drivers of Digital Transformation

## Knowledge Check

### Business Drivers of Digital Transformation

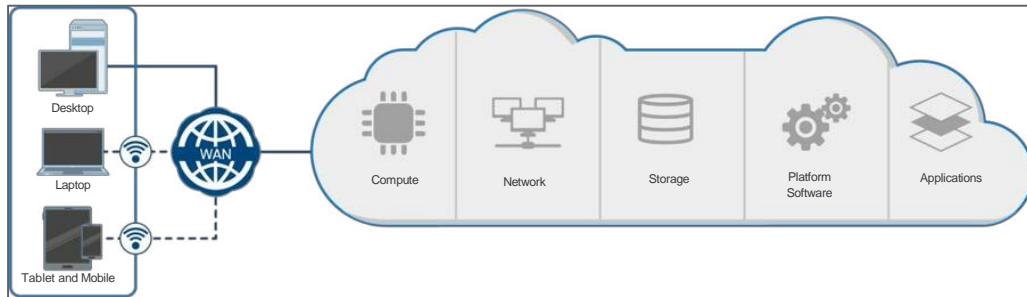
# Cloud Computing

## Cloud Computing

## Cloud Computing Overview

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services).

It can be rapidly provisioned and released with minimal management effort or service provider interaction.



***Cloud Infrastructure***

### Notes:

- The term “cloud” originates from the cloud-like bubble that is commonly used in technical architecture diagrams to represent a system. This system may be the Internet, a network, or a compute cluster.
- In cloud computing, a cloud is a collection of IT resources, including hardware and software resources. You can deploy these resources either in a single data center, or across multiple geographically dispersed data centers that are connected over a network.
- A cloud service provider is responsible for building, operating, and managing cloud infrastructure. The cloud computing model enables consumers to obtain IT resources internally.
- A cloud service is a combination of hardware and software resources that are offered for consumption.
- The cloud infrastructure contains IT resources pools that can be provisioned to a consumer. Resources are returned to the pool when the consumer releases them.

## Cloud Computing Characteristics

### Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability. At some level of abstraction it is appropriate to the type of service such as, storage, processing, bandwidth, and active user accounts.

Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the used service.



### Resource Pooling

The provider's computing resources are pooled to serve multiple consumers using a multitenant model. Uses different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (for example, country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth. – NIST



## Rapid Elasticity

Capabilities can be elastically provisioned and released, sometimes automatically, to scale rapidly outward and inward commensurate with demand.

To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

## On-demand Self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.



### Broad Network Access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (such as, mobile phones, tablets, laptops, and workstations).



## Cloud Computing Benefits



**1:** Cloud computing provides the capability to provision IT resources quickly and at any time, thereby considerably reducing the time required to deploy new applications and services.

- This enables businesses to reduce the time-to-market and to respond more quickly to market changes.

**2:** Cloud computing enables the consumers to rent any required IT resources based on the pay-per-use or subscription pricing.

- This reduces a consumer's IT capital expenditure as investment is required only for the resources needed to access the cloud services.

**3:** Cloud computing has the ability to ensure resource availability at varying levels depending on the consumer's policy and application priority.

**4:** In cloud computing, consumers can unilaterally and automatically scale IT resources to meet the workload demand.

- This is significantly more cost-effective than buying new IT resources that are only used for a short time or only during specific periods.

## Cloud Computing

**5:** It is possible for IT services to be rendered unavailable due to causes, such as natural disasters, human error, technical failures, and planned maintenance.

- Through the use of cloud business continuity solutions, an organization can mitigate the impact of downtime and can recover from outages that adversely affect business operations.

**6:** Cloud computing enables collaboration between disparate groups of people by allowing them to share resources and information and access them simultaneously from any location.

**7:** Moreover, when an organization uses cloud services, their infrastructure management tasks are reduced to managing only those resources that are required to access the cloud services.

**8:** In cloud computing, applications and data reside centrally and can be accessed from anywhere over a network from any device such as desktop, mobile, and thin client.

- Eliminates a consumer's dependency on a specific end-point device.
- Enables Bring Your Own Device (BYOD), which is a recent trend in computing, whereby employees are allowed to use non-company devices as business machines.

## Cloud Service Models

A cloud service model specifies the services and the capabilities that are provided to consumers. In SP 800-145, NIST classifies cloud service offerings into three primary models:

- Infrastructure as a Service (IaaS)<sup>3</sup>
  - Platform as a Service (PaaS)<sup>4</sup>
  - Software as a Service (SaaS)<sup>5</sup>
- 

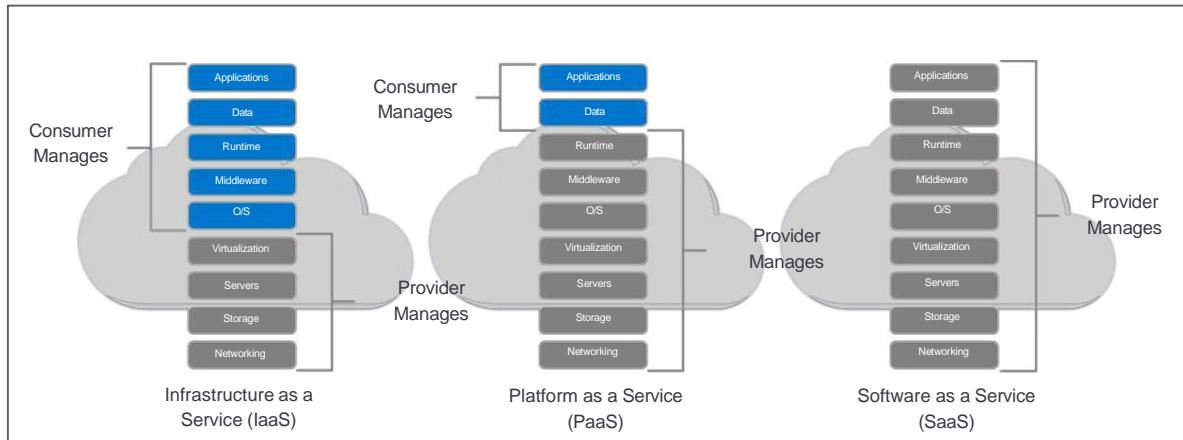
<sup>3</sup> Provide capability to the customer to obtain infrastructure components such as servers, storage, and network. Also, enables consumers to deploy and run software, including OS and applications. Examples of IaaS are: Amazon EC2, S3, Google Compute Engine.

<sup>4</sup> Capability provided to the consumer to deploy consumer-created or acquired applications on the provider's infrastructure. Consumers have control over deployed applications and application hosting environment configurations.

Examples of PaaS are: Google App Engine, AWS Elastic Beanstalk, Microsoft Azure SQL.

<sup>5</sup> Capability provided to the consumer to use provider's applications running in a cloud infrastructure. Complete stack including application is provided as a service. Application is accessible from various client devices. For example, through a thin-client interface such as web browser. Examples of SaaS are: Salesforce.com, Google Apps, and Microsoft 365.

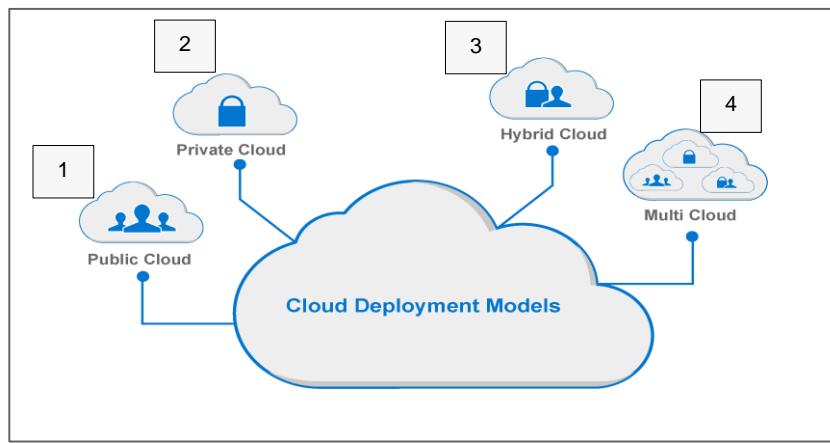
# Cloud Computing



*Cloud Service Models*

## Cloud Deployment Models

- A cloud deployment model provides a basis for how cloud infrastructure is built, managed, and accessed.
- Each cloud deployment model may be used for any of the cloud service models: IaaS, PaaS, and SaaS.
- Different deployment models present several tradeoffs in terms of control, scale, cost, and availability of resources.



**1:**

- Public cloud services may be free, subscription-based, or provided on a pay-per-use model. A public cloud provides the benefits of low upfront expenditure on IT resources and enormous scalability.
- Some concerns for the consumers include network availability, risks associated with multitenancy, visibility, and control over the cloud resources and data, and restrictive default service levels.

**2:**

- Many organizations may not want to adopt public clouds due to concerns related to privacy, external threats, and lack of control over the IT resources and data. When compared to a public cloud, a private cloud offers organizations a greater degree of privacy and control over the cloud infrastructure, applications, and data.
- There are two variants of private cloud: on-premise and externally hosted.

## Cloud Computing

**3:**

- A composition of two or more distinct cloud infrastructures (private or public) that remain unique entities, but are bound by standardized or proprietary technology. It enables data and application portability (for example, cloud bursting for load balancing between clouds.)

**4:**

- To create the best possible solution for their businesses, organizations want to choose different public cloud service providers. To achieve this goal, some organizations have started adopting a multicloud approach.
- The drivers for adopting multicloud approach include avoiding vendor lock-in, data control, cost savings, and performance optimization. This approach helps to meet the business demands since sometimes no single cloud model can suit the varied requirements and workloads across an organization.

## Cloud Computing: Use Cases

### Cloud Bursting

- Provisioning resources for a limited time from a public cloud to handle peak workloads.
- Public cloud can be used to scale your network and resources to manage and handle peak seasonal traffic. When the traffic goes down, you can terminate your infrastructure within the cloud.
- You only pay for what you use, when you use it.



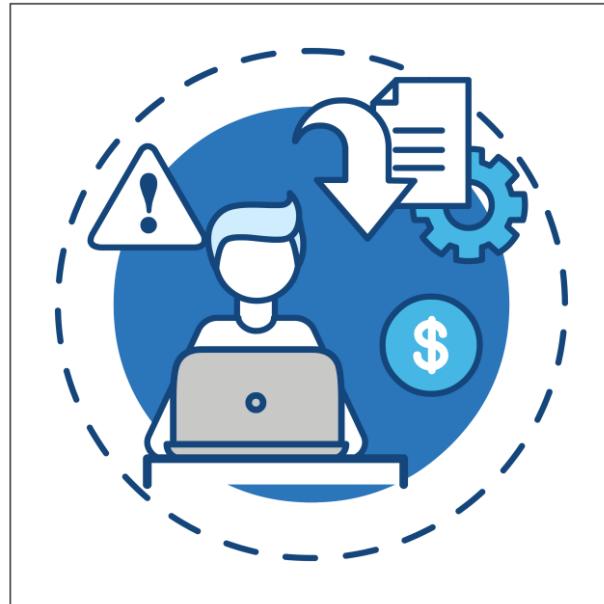
### VDI and DaaS

- With the frequent growth in mobile workforce, employees are progressively bringing their own devices. Virtual Desktop Infrastructure (VDI) and Desktop as a Service (DaaS) have emerged as a way for organizations to standardize security and content access across devices.
- VDI and DaaS helps to increase data and application availability, because they are hosted in the cloud and can be easily accessed from any device.



## Disaster Recovery

- Adopting cloud for a DR solution can provide cost benefit, scalability and faster recovery of data
- By having a standby site in the cloud for DR purposes, failover is quick and easy. Also, there is no need to build and maintain separate infrastructure.



## Application Development and Testing

- Developing and testing applications in the public cloud before launching them.
  - In the cloud, you can switch environments on and off. Unlike traditional infrastructures, the cloud allows you to create, deploy, and terminate environments anytime you want.
  - With just a few clicks, you could quickly set up a development environment to improve your time to market.



## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Identify the service of cloud computing in which the resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
  - a. Resource pooling
  - b. On-demand self-service
  - c. Measured services
  - d. Rapid elasticity

Big data

Big data

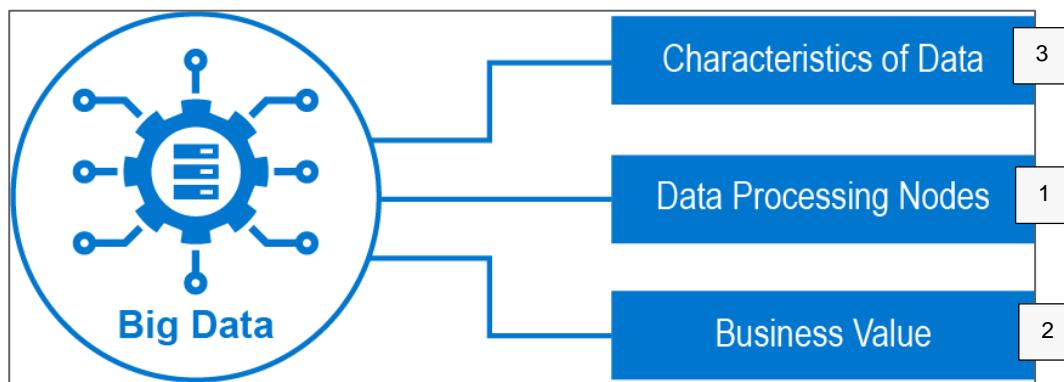
Big data

## Big Data

## Big Data Overview

**Big Data:** Information assets whose high volume, high velocity, and high variety require the use of new technical architectures and analytical methods to gain insights and derive business value.

The definition of big data has three principal aspects, as shown in the image.

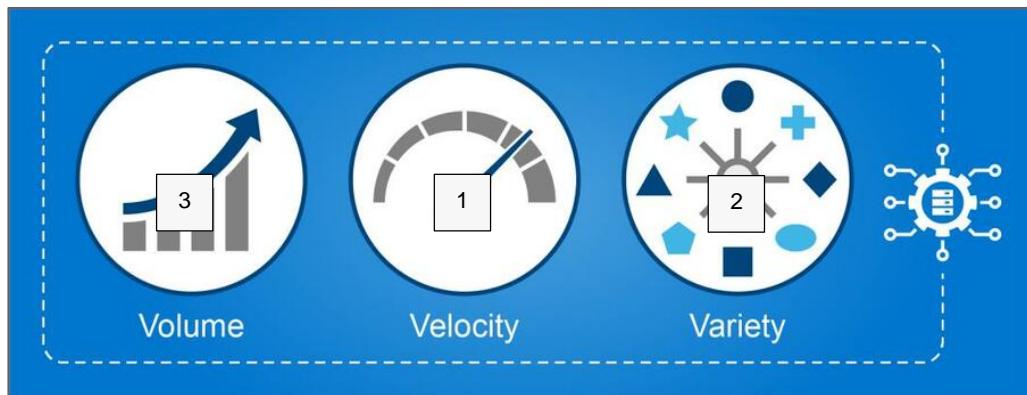


**1:** Big data exceeds the storage and processing capability of conventional IT infrastructure and software systems. It not only needs a highly scalable architecture for efficient storage, but also requires new and innovative technologies and methods for processing.

**2:** Big data analytics has tremendous business importance to organizations. Searching, aggregating, and cross-referencing large datasets in real-time or near-real time enables gaining valuable insights from the data. It enables better data-driven decision making.

**3:** Big data includes datasets of considerable sizes containing both structured and unstructured digital data. Apart from its size, the data gets generated and changes rapidly, and also comes from diverse sources.

## Characteristics of Big Data



1:

- Velocity is the rate at which data is produced and changes, and also how fast the data must be processed to meet business requirements.
- Today, data is generated at an exceptional speed, and real-time or near-real time analysis of the data is a challenge for many organizations.
- It is essential for the data to be processed and analyzed, and the results to be delivered in a timely manner.
- An example of such a requirement is real-time face recognition for screening passengers at airports.

2:

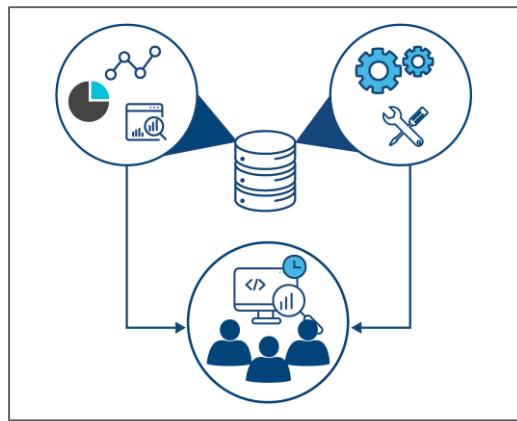
- Variety is the diversity in the formats and types of data.
- Data is generated by numerous sources in various structured and unstructured forms.
- Organizations face the challenge of managing, merging, and analyzing the different varieties of data in a cost-effective manner.
- Combination of data from various data sources and in various formats is a key requirement in Big Data analytics.
- An example of such a requirement is combining the many medical records of a particular patient with various published medical research to find the best treatment.

**3:** The word “Big” in big data is the massive volume of data. Organizations are witnessing an ever-increasing growth in data of all types, such as:

- Transaction-based data stored over the years.
- Sensor data.
- Unstructured data streaming in from social media.

This growth in data is reaching Petabyte—and even Exabyte—scales. The excessive volume not only requires substantial cost-effective storage, but also increases challenges in data analysis.

## Big Data Analytics



*Big Data Analytics (click image to enlarge)*

- With big data analytics, organizations can use their Big data to:
  - Uncover new, emerging trends.
  - Identify potential business opportunities.
  - Discover new ways to gain competitive advantages.
- Big data demands an approach to analytics that is flexible, accessible, and fast.
- To maximize the value of Big data, analysts:
  - Leverage data lakes that can store a massive amount of data.
  - Apply statistical and machine learning techniques to deliver predictive analytics.

## Big Data: Use Cases

### Healthcare

Provides consolidated diagnostic information and enable healthcare providers to:

- Analyze patient data.
- Improve patient care and outcomes.
- Minimize errors.
- Increase patient engagement.
- Improve operations and services.

These solutions also enable healthcare providers to monitor patients and analyze their experiences in real time.



### Finance

Big Data analytics is used to detect fraudulent credit card transaction in near-real time.



## Retail and eCommerce

Provides valuable insights for competitive pricing, anticipating future demand, effective marketing campaigns, optimized inventory assortment, and improved distribution.

- Enables businesses to provide optimal prices and services to customers.
- Improves operations and revenue.



## Social Network Analysis

- Enables valuable insights from the data that is generated through social networking.
- Enables the discovery and analysis of communities, personalization for solitary activities (for example, search) and social activities (for example, discovery of potential friends).



## Knowledge Check

## Knowledge Check

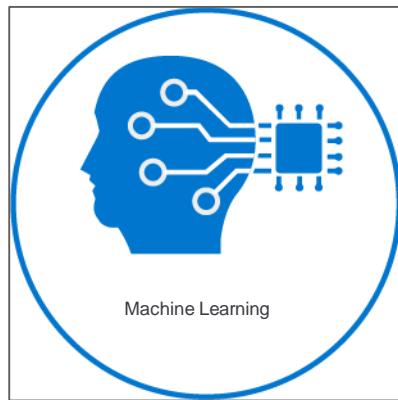
### Knowledge Check

1. Which characteristic of Big Data refers to the diversity in the formats and types of data?
  - a. Volume
  - b. Velocity
  - c. Variety
  - d. Veracity

# Artificial Intelligence and Machine Learning

## Artificial Intelligence and Machine Learning

## AI/ML Overview



- Data is growing at an astronomical rate, and it is impossible to take full advantage of it manually to get insights.
- Automation can provide faster, better, and deeper data insights. With the advancement of systems and modern technologies, intelligent machines are being built to automatically learn from data and to make decisions.
- As cloud computing and big data technologies generate voluminous data, these intelligent machines help to process the data in real time.

Artificial intelligence and machine learning<sup>6</sup> are two intertwined concepts that help to build this human-like ability into systems.

---

<sup>6</sup> The process of ‘training’ the machine, feeding large amounts of data into algorithms that give it the ability to learn how to perform the task without being explicitly programmed. Instead of writing a program, a machine is provided with data. With the help of algorithms, machines learn from the data and complete a specific task. When the machine is provided with a new dataset, it adapts to it by learning from previous experiences to produce reliable outputs.

## Artificial Intelligence and Machine Learning

- Artificial Intelligence (AI) is an umbrella term, while machine learning techniques make AI possible.
- AI technologies enable intelligent systems that work and behave like humans.

## AI/ML Machine Learning Methods



*To view the video about machine learning methods, click [here](#).*

A machine learning process involves creating mathematical and statistical algorithms that can accept input data and use some sort of analysis to predict the output.

- First step is to collect the datasets for analysis.
- Once the data is collected:
  - Select the type of learning method to be used, then build a model.
  - Train the model with test datasets and improvise the model accordingly for future decision making.
- There are many ways in which machines learn. Most machine learning methods can be classified into the following three types:
  - Supervised
  - Unsupervised
  - Reinforcement

Knowledge Check

## Knowledge Check

## Knowledge Check

1. Which learning algorithm is enabled to interact with its environment and produce results that are based on a trial and error method?
  - a. Supervised learning
  - b. Unsupervised learning
  - c. Reinforcement learning
  - d. Deep learning

Internet of Things (IoT)

## Internet of Things (IoT)

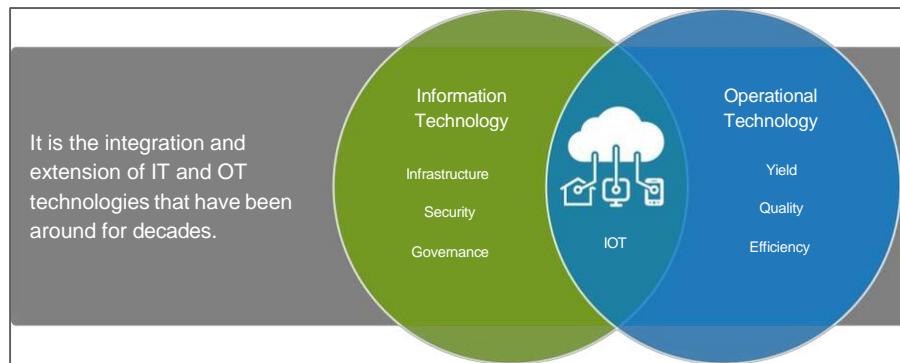
## Internet of Things (IoT)

### Internet of Things (IoT) Overview

The Internet of Things (IoT) is fundamentally changing how users interact with the physical world. By connecting everything from industrial equipment to cars to the natural environment, users can know things that were previously unknowable.

IoT is an ecosystem where sensors, devices, and equipment are connected to a network and can transmit and receive data for tracking, analysis, and action. Some examples are:

- **Wearable gadgets** – smartwatches and fitness activity trackers.
- **Electronic sensors** – temperature sensors and heart monitoring implants.
- **Household appliances** – TV, thermostats, and lighting.



## IoT Architecture

An IoT implementation requires a proper understanding of its components and all IoT devices and applications communication using various standards.

The main components of IoT architecture are:

- Smart things<sup>7</sup>
  - Gateways<sup>8</sup>
  - Middleware<sup>9</sup>
  - Applications<sup>10</sup>
- 

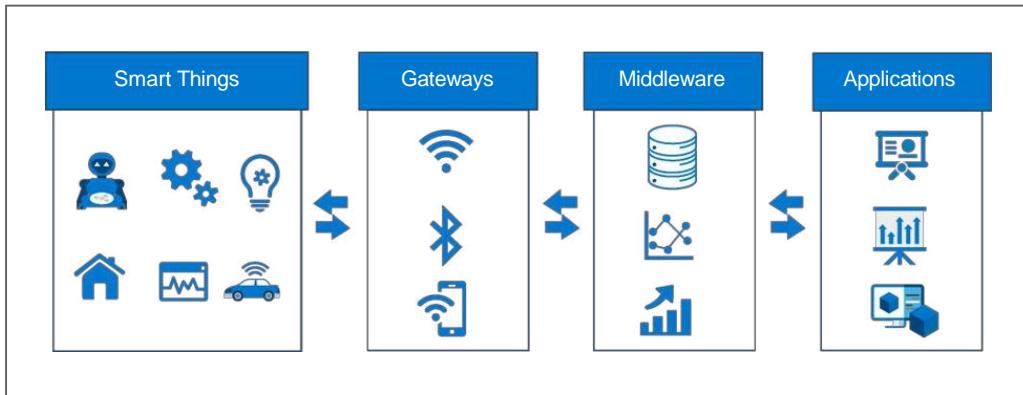
<sup>7</sup> Devices that collect, analyze, and transmit data.

<sup>8</sup> Gateways are devices that manage data traffic between networks. In IoT, these gateway devices can also be designed to analyze and secure the data before transmitting for further processing.

<sup>9</sup> Enables connectivity for huge numbers of diverse Things by providing a connectivity layer for sensors and also for the application layers that provide services that ensure effective communications among software.

<sup>10</sup> To monitor and control the smart things, applications enable the connection of end users or devices to an IoT device.

## Internet of Things (IoT)



*Internet of Things Architecture*

## Internet of Things: Use Cases

### Home Automation

- The use of IoT has entered the residential environment with the introduction of smart home technology.
- Various electronic objects at home such as air conditioner, lights, refrigerators, security cameras, kitchen stoves can be connected to the Internet with the help of sensors.



### Smart Cities

- The smart cities concept highlights the need to enhance the quality of life of the citizens using smart public infrastructure.
- Enables optimization of power usage, efficient water supply, manage waste collections, reliable public transportation using IoT sensors.



## Internet of Things (IoT)

### Wearables

With the use of wearables such as smart watches on people, IoT sensors can collect data about the users regarding their health, heartbeat, and exercise patterns.

### Manufacturing

In manufacturing, IoT enables efficient material flow, inventory control, and process monitoring to reduce costs and improve quality.



## Knowledge Check

## Knowledge Check

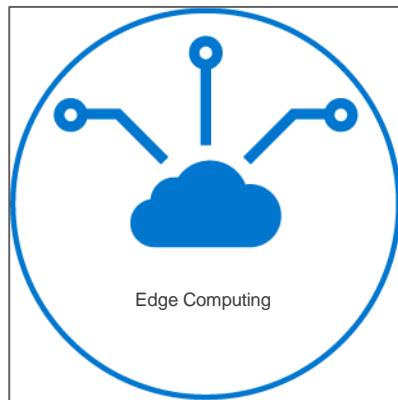
### Knowledge Check

1. Which IoT architecture component enables connectivity for huge numbers of diverse things through connectivity layer for sensors?
  - a. Smart things
  - b. Gateways
  - c. Middleware
  - d. Applications

# Edge Computing

## Edge Computing

## Edge Computing Overview



The Edge exists wherever the digital and physical worlds intersect and data is securely generated, collected, processed and used to create new value.

- The modern Edge is an interconnected system of geographically distributed compute and data capabilities working together as a common platform.
  - The edge platform places these capabilities in proximity to the control and ingest points.
- The modern edge addresses immense data growth, mission critical applications, low-latency responses, and varied communications access, such as 5G.

### Edge Computing: Use Cases

#### Healthcare

The increasing volume of medical data and the need to envision smarter digital healthcare systems led to adoption of edge computing.

Edge enables digital transformation across multiple areas of healthcare by:

- Providing a better patient experience at a lower cost, with connected healthcare systems that deliver real-time access to patient insights and support advanced data analytics.
- Enabling fusion of diverse data feeds from multiple departments and sites.
- Improving organizational agility, clinical outcomes, and professional staff effectiveness.
- Improving outcomes through the use of telemedicine.
- Providing data-driven preventative and predictive medicine.

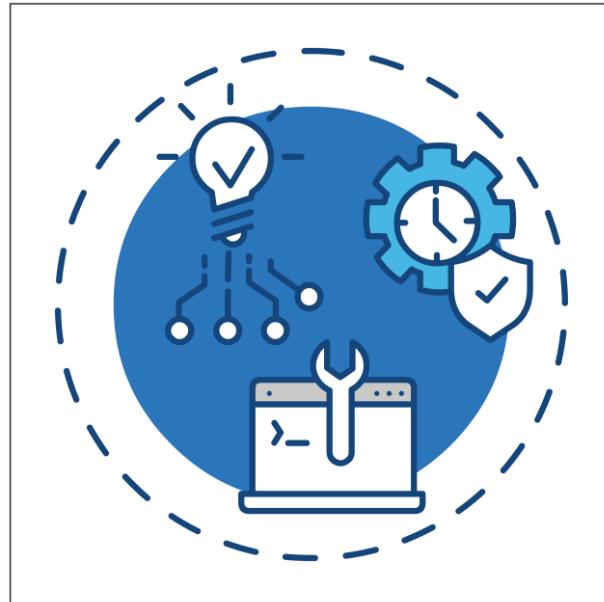


## Energy

Within the evolving energy industry, companies are looking for new ways to optimize operations and management. Edge plays an important role in turning enormous volumes of high-velocity data into actionable intelligence by performing advanced analytics at the source or point of collection.

Edge helps companies to:

- Manage increasingly complex grids.
- Enable real-time demand forecasting, affordable and reliable service delivery, enhanced security, and increased customer satisfaction.
- Track energy transactions, improve security, enable efficient resource allocation, and deliver new business models.
- Predict problems, deploy resources efficiently, and avoid outages.
- Modernize physical security to keep facilities and employees safe



## Edge Computing

### Retail

Implementation of Edge computing in retail drives improved decision making by collecting, aggregating, and analyzing data.

In retail, edge helps to:

- Personalize customer experiences by analyzing buying behavior.
- Implement advanced loss prevention that can detect fraudulent actions.
- Utilize predictive inventory and supply chain control.
- Drive revenue by predicting best sellers.



### Manufacturing

Edge computing helps to transform manufacturers' operations, by consolidating and simplifying diverse infrastructure, adding intrinsic security, and generating insights at the point of data generation.

- Provide operational intelligence to increase agility and efficiency while reducing costs and downtime.
- Reduce failures by identifying issues before they impact production, which minimizes down time and improves asset optimization.



## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Which of the following is an interconnected system of geographically distributed compute and data capabilities working together as a common platform?
  - a. Edge
  - b. 5G
  - c. IoT
  - d. Big data

## 5G

## 5G Overview



5G is a fifth-generation mobile network after 4G networks. 5G wireless mobile technology promises to:

- Enable a fully mobile and connected society virtually including objects, devices, and machines.
- Empower socio-economic transformations, enhancing productivity, sustainability, efficiency, and overall well-being of communities.

With the advent of 5G, upward industries will use the enhanced technical capacity and tighter integration to trigger new products and services.

5G creates an ecosystem for technical and business innovation that will fundamentally alter entire upward markets such as automobiles, energy, food and agriculture, smart city management, governance, health sector, production, transportation, and many more.

## 5G Features



*5G network features (click image to enlarge)*

5G is a revolution of mobile technology. The features and its reliability bring tremendous growth in connectivity, mobile traffic capacity, and new capabilities that enhance performance by providing greater throughput, lower latency, ultra-high reliability, higher connectivity density and an expanded range of mobility. 5G network features:

- Automate many network behaviors.
- Unite wireless, wireline, and satellite services in the same house.
- Offer platform-enabling services for upward markets.
- Deliver services at lower cost.
- Deploy multiple virtual 5G networks on ordinary infrastructure using network slicing.
- Extreme broadband adaptivity with peaks of 20 Gbps.

## 5G: Case Study



### Situation

As we enter the new data era, by 2025, the total amount of digital data created worldwide will rise to 175 zettabytes, with 30% of data processed in real time.

- Data will continue to grow and the current network infrastructure is insufficient.
- In the move to 5G, operators need to rapidly scale out networks to take advantage of the efficiencies and carefully invest in infrastructure that has an immediate impact while setting the stage for future service-enablement and revenue creation.

### Challenge

As such, there is no one-size-fits-all approach to buying network equipment. This reality is compounded in an era of disaggregation with software-defined networking and open interfaces slowly gaining ground on single-vendor stacks.

- A compounding challenge is the ongoing move to disaggregate hardware and software as a way for operators to deliver compelling services combining 5G, edge compute and more.
- Operators must deliver differentiated enterprise services combining the power of 5G and edge computing, to record meaningful 5G service revenues.

## Solution

Dell partnered with World-Wide Technology (WWT) to help operators streamline validation, procurement and deployment.

- Dell Technologies partnered with CSPs around the world to make emerging technologies like 5G and edge computing opportunities. The vision is to transform the network through workload virtualization, software-defined infrastructure, and open architectures.
- World-Wide Technologies uses a proven and innovative approach to help customers discover, evaluate, architect, and implement advanced technology lab testing in the Advanced Technology Center and deploy their solutions rapidly through global integration centers.

### Reference:

[5G Network Connectivity and Infrastructure | Dell Technologies US](#)

Knowledge Check

## Knowledge Check

## Knowledge Check

1. Which of the following is a feature of 5G network?

- a. Ultra low-density
- b. Ultra high-energy
- c. Ultra high-complexity
- d. Ultra low-latency

## Concepts in Practice

## Concepts in Practice

### APEX Hybrid Cloud

Dell Technologies hybrid cloud solutions provide a simplified and consistent approach to the cloud that can be tailored for specific organizations to reach new levels of agility, reliability, data protection and control. Hybrid cloud solution also provides:

- **A single vendor experience** with consistent SLAs across all cloud workloads and single-vendor support.
- **Unparalleled breadth of capabilities** with a range of cloud solutions that enable greater innovation and provide the flexibility of cost-efficient, multiple cloud consumption models.
- **A consistent experience and common management tools** across all clouds, enabling IT teams to choose the optimal mix of public, private and edge cloud resources.
- **Support for all major cloud partners**, with the ability to extend hybrid cloud solutions to the world's broadest cloud ecosystem that includes more than 4,200 cloud providers like AWS, Azure and Google Cloud Platform.

VMware Cloud Foundation on VxRail is the foundation for APEX Hybrid Cloud. It delivers a simple and direct path to modern apps and the hybrid cloud with one, complete, automated platform.

Deep integration between VxRail and VMware Cloud Foundation combines operational transparency, automation, support, and serviceability capabilities for a turnkey hybrid cloud experience.



## Dell Edge Gateway

The Dell Edge Gateway allows you to connect (wired or wireless) to network enabled devices and manage them remotely in your existing network ecosystem. The Dell Edge Gateway can:

- Mount on a wall or DIN rail at the edge of the network enabling you to collect, secure, analyze, and act on data from multiple disparate devices and sensors.
- Help to connect, extract, and analyze data from both legacy and modern systems with the help of expanded I/O. It supports diverse communication protocols through certified independent software vendor (ISV) middleware.
- Perform analytics locally, close to the devices and sensors generating data. It sends only meaningful data to the cloud or data center or to a master gateway—instead of gorging on bandwidth and wasting money transmitting every unprocessed dataset.

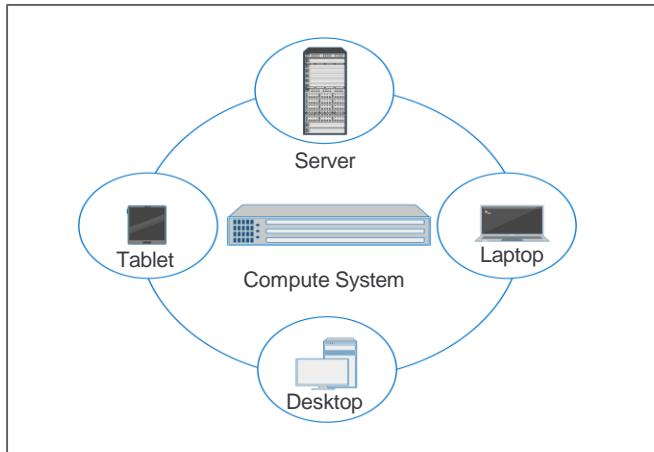


# Modern Data Center Environment

## Modern Data Center Environment

## Compute Systems

## Compute Systems

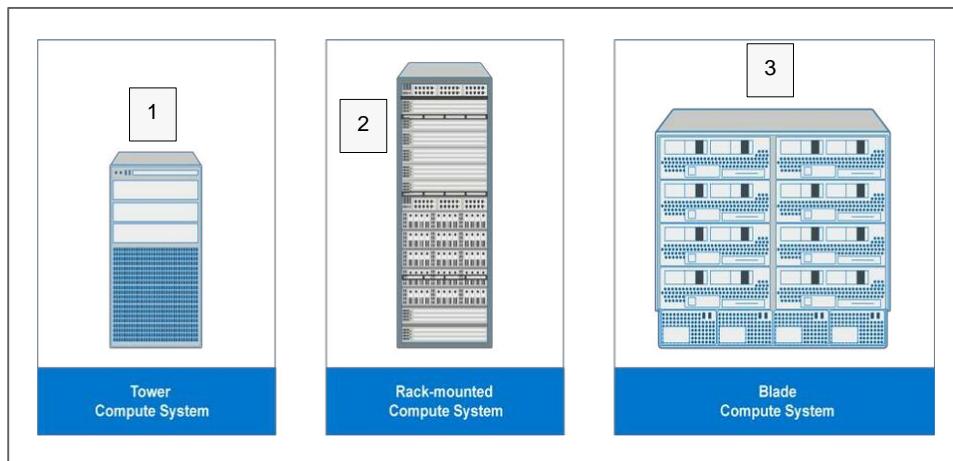


- A compute system is a computing device (combination of hardware, firmware, and system software) that runs business applications.
  - Examples of compute systems include physical servers, desktops, laptops, and mobile devices.
- A compute system's hardware consists of processor(s), memory, internal storage, and I/O devices.
- The logical components of a compute system include the operating system (OS), file system, logical volume manager, and device drivers.
- In a modern data center, applications are typically deployed on compute clusters<sup>11</sup> for high availability and for balancing computing workloads.

---

<sup>11</sup> A compute cluster is a group of two or more compute systems that function together, sharing certain network and storage resources, and logically viewed as a single system.

## Types of Compute Systems



**1:** A tower compute system is placed within an upright, standalone structure call a "tower", which looks similar to a desktop cabinet.

Tower compute systems typically have individual monitors, keyboards, and mice. These towers occupy significant floor space and require complex cabling when deployed in a data center.

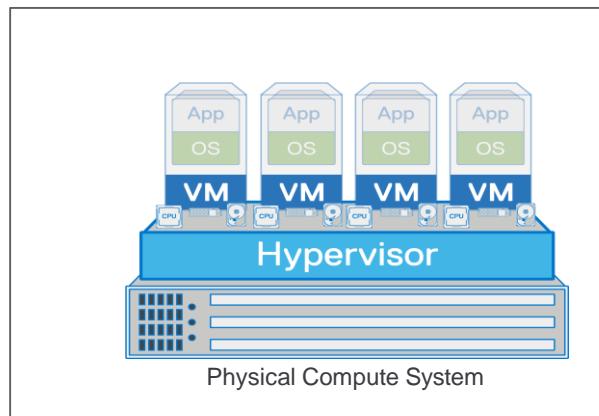
**2:** Rack-mounted compute systems consist of multiple servers placed into an enclosure called a rack. The rack contains multiple servers stacked vertically, thereby simplifying network cabling, consolidating network equipment, and reducing the floor space use.

**3:** A blade compute system consists of several blade servers installed into one or more chassis. Also known as modular servers.

A blade server is a printed circuit board containing only core processing components, such as CPU(s), memory, integrated network controllers, storage drive, and essential I/O cards and ports. Providing integrated power, cooling, and networking, each chassis has multiple slots to hold multiple blade servers.

The modular design of the blade servers makes them smaller, which minimizes the floor space requirements, increases the compute system density and scalability, and provides better energy efficiency as compared to the tower and the rack servers.

### Compute Virtualization



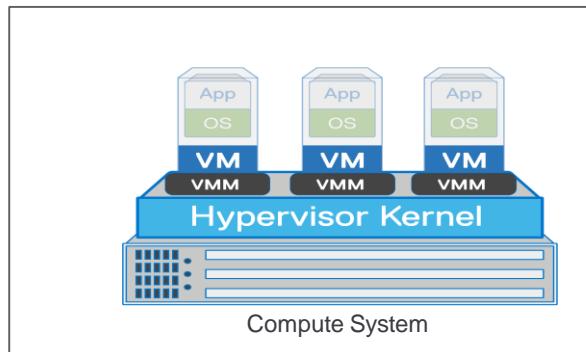
**Compute virtualization** is a technique of abstracting the physical compute hardware from the operating system and applications enabling multiple operating systems to run concurrently on a single or clustered physical compute system(s).

#### Notes:

- Compute virtualization enables the creation of virtual compute systems called virtual machines (VMs). Each VM runs an OS and applications, and is isolated from the other VMs on the same compute system.
- Compute virtualization is achieved by a hypervisor, which is virtualization software that is installed on a physical compute system.
  - The hypervisor provides virtual hardware resources, such as CPU, memory, storage, and network resources to all the VMs. Depending on the hardware capabilities, several VMs can be created on a single physical compute system.
- A VM is a logical entity; but to the OS running on the VM, it appears as a physical compute system, with its own processor, memory, network controller, and disks. However, all VMs share the same underlying physical hardware of the compute system. The hypervisor allocates the compute system's hardware resources dynamically to each VM.

## Hypervisor

A hypervisor<sup>12</sup> is software that allows multiple operating systems (OSs) to share and run concurrently on a single compute system.



- Each Virtual Machine (VM) is isolated from the other VMs on the same physical compute system. Therefore, the application running on one VM does not interfere with those running on other VMs.
  - Isolation also provides fault tolerance so that if one VM crashes, the other VMs remain unaffected.
- Each VM is assigned a virtual machine manager (VMM). VMM abstracts the physical hardware and presents it to the VM.
- The compute system on which a hypervisor is running is called a host machine and each VM is called a guest machine.
- The OS that is installed on a guest machine is called a guest OS<sup>13</sup>.

---

<sup>12</sup> The hypervisor provides a compute virtualization layer that abstracts the physical hardware of a compute system from the OS and enables the creation of multiple VMs.

<sup>13</sup> An application can run on the guest OS.

## Virtual Machine

A Virtual Machine (VM) is a logical compute system with virtual hardware on which a supported guest OS and application run. From the perspective of the guest OS, a VM appears as a physical compute system.

- A VM consists of files such as - Configuration File<sup>14</sup>, Virtual Disk File<sup>15</sup>, Memory State File<sup>16</sup> and Log File<sup>17</sup>.
- The image shows the typical virtual hardware components of a VM.
  - This includes virtual CPU(s), virtual motherboard, virtual RAM, virtual disk, virtual network adapter, optical drives, serial and parallel ports, and peripheral devices.

---

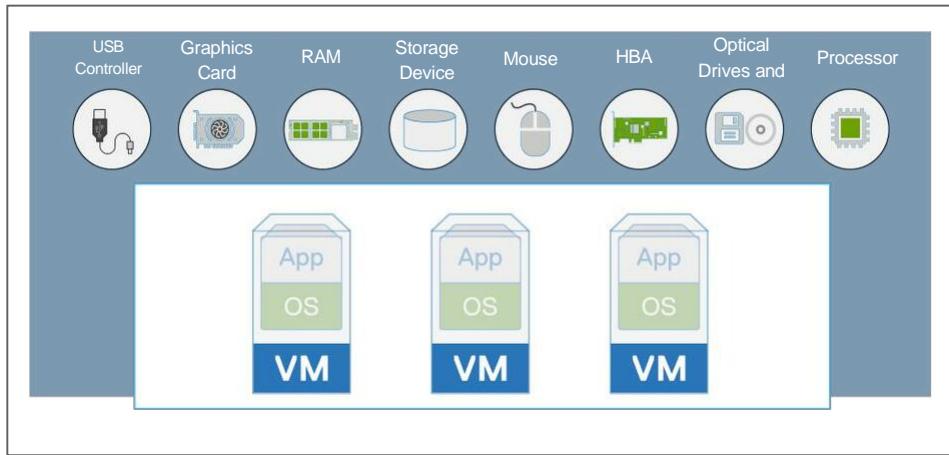
<sup>14</sup> Stores the VM's configuration data, including VM name, location, BIOS information, guest OS type, number of CPUs, memory size, number of adapters and associated MAC addresses, and SCSI controller type.

<sup>15</sup> Stores the content of a VM's disk drive. A VM can have multiple virtual disk files, each of which appears as a separate disk drive to the VM.

<sup>16</sup> Stores the memory contents of a VM and is used to resume a VM that is in a suspended state.

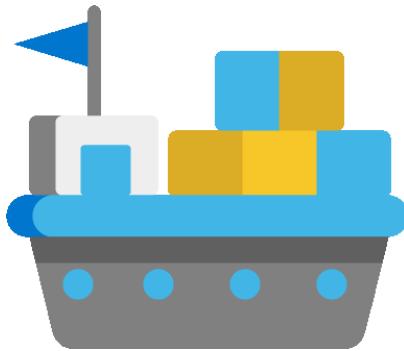
<sup>17</sup> Used to keep a record of the VM's activity and is often used for troubleshooting purposes.

## Compute Systems



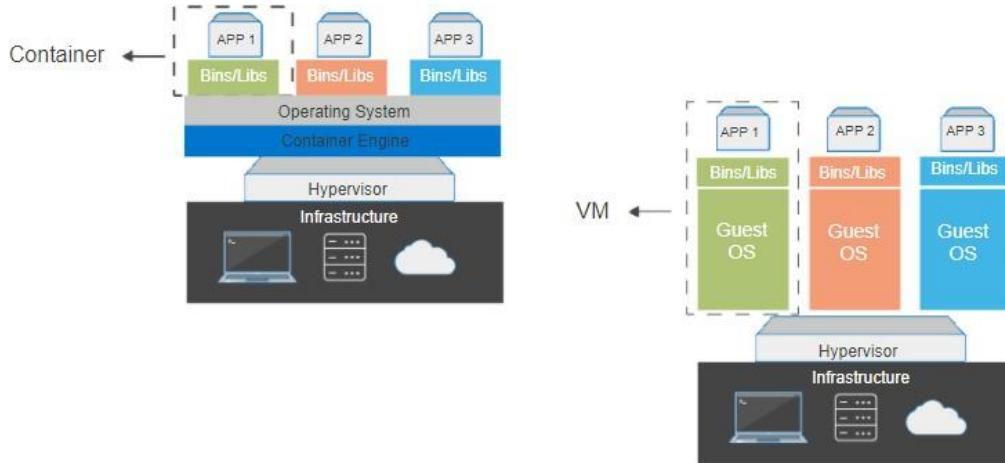
*Hardware components of a virtual machine*

## Containers



- Containerization is an operating system-level virtualization method that simplifies application deployment and requires fewer resources than virtual machines.
- Containers are application-centric methods that:
  - Delivers microservices by providing portable, isolated virtual environments for applications to run without interference from other running applications.
  - Bundles applications with the software libraries that they depend on, allowing developers to create “build once, run anywhere” code making applications very portable.
  - Becomes the norm for modern applications and cloud-native applications.

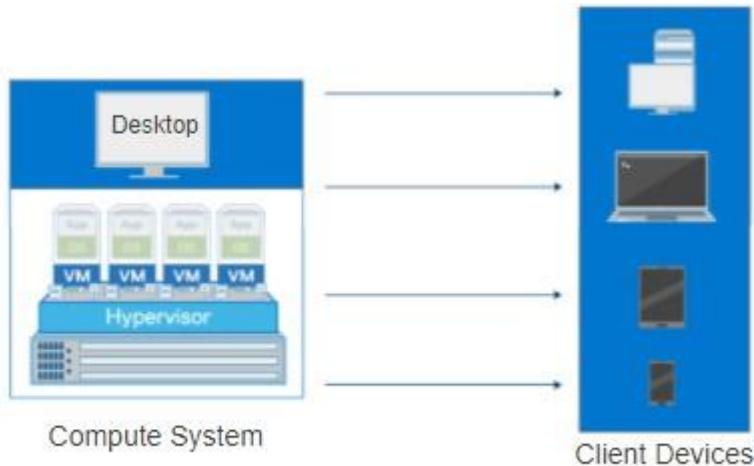
## Containers vs. VMs



Container vs. VM

Containers	VMs
Shared operating system	Separate operating system
Small image footprint, (MB)	Large image footprint, (GB)
Quick start times	Full boots
Stateless	Stateful
Easily transportable	Not easily portable, (exports/conversions/etc)

## Desktop Virtualization



*Desktop virtualization*

**Desktop virtualization** is a technology that decouples the OS, applications, and user state from a physical compute system to create a virtual desktop environment that can be accessed from any client device.

Desktop virtualization benefits include:

- Simplified desktop infrastructure management<sup>18</sup>

---

<sup>18</sup> Desktop virtualization simplifies desktop infrastructure management, and creates an opportunity to reduce the maintenance costs. New virtual desktops can be configured and deployed faster than physical machines. The patches, updates, and upgrades can be centrally applied to the OS and applications. This process simplifies or eliminates many redundant, manual, and time-consuming tasks.

- Improved data protection and compliance<sup>19</sup>
  - Flexibility of access<sup>20</sup>
- 

<sup>19</sup> Applications and data are located centrally, which ensures that business-critical data is not at risk if there is loss or theft of the device. Virtual desktops are also easier to back up compared to deploying backup solutions on end-point devices.

<sup>20</sup> Desktop virtualization enables users to access their desktops and applications without being bound to a specific end-point device. The virtual desktops can be accessed remotely from different end-point devices. These benefits create a flexible work scenario and enables user productivity from remote locations. Desktop virtualization also enables Bring Your Own Device (BYOD), which creates an opportunity to reduce acquisition and operational costs.

## Virtual Machine and Container Lab Demo



*To view the demo of creating VM and Docker Container, click [here](#).*

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Which compute system contains multiple servers stacked vertically in an enclosure?
  - a. Tower
  - b. Rack-mounted
  - c. Blade
  - d. Edge

## Applications

## Applications

## Traditional Applications

Traditional applications are designed for desktop first, and then extended to other devices as necessary.

- Separate interfaces based on the device are often required.
- Scalability is achieved through a stateful design approach, using a monolithic architecture that can be vertically scaled.
  - For resilience, also known as availability, traditional applications most typically rely on highly available infrastructure with redundant components and automated recovery to failure.
- Most of the applications are monolithic where the applications are developed as tightly coupled code, installable as a single package.
- In this environment, acquisition and provisioning of new resources commonly follow a rigid process (Ticket-based).
  - The process includes approvals from the concerned authorities and most of these IT operations involved manual intervention.

## Cloud-Native Applications

Modern applications consist of a set of business-related functional parts, called microservices, that are assembled with specific rules and best practices. Cloud-native applications:

- Requires a dynamic modern infrastructure platform with the attributes such as on-demand self-service, resource pooling, virtualization, accessibility, and scalability.
- Enables services to be delivered in hours and not weeks or months that are common in the new world of a digital business.
- Supports predictive, and reactive, scaling algorithms using live performance measures to dynamically scale out.



*New standards for cloud-native applications as per IDC FutureScape 2020*

## Application Virtualization

**Application virtualization** is a technique of decoupling an application from the underlying computing platform (operating system and hardware) to enable the application to be used on a compute system without installation.

An application is either delivered from a remote compute system, or encapsulated in a virtualized container.

Application virtualization benefits are:

- Simplified application deployment and management<sup>21</sup>
  - Eliminate OS modifications<sup>22</sup>
  - Resolve application conflicts and compatibility issues<sup>23</sup>
  - Simplified OS image management<sup>24</sup>
  - Flexibility of application access<sup>25</sup>
- 

<sup>21</sup> Provides a solution to meet an organization's need for simplified and improved application deployment, delivery, and manageability.

<sup>22</sup> Provides additional security, and protects the OS from potential corruptions and problems that may arise due to changes to the file system and registry.

<sup>23</sup> Enables the use of conflicting applications on the same end-point device. It also enables the use of applications that otherwise do not execute on an end-point device due to incompatibility with the underlying computing platform.

<sup>24</sup> Simplifies OS image management. Since application delivery is separated from the OS, there is no need to include "standard" applications in end-point images. As a result, managing images is simpler, especially in the context of OS patches and upgrades.

## Course Completion

---

<sup>25</sup> Enables an organization's workforce and customers to access applications hosted on a remote compute system from any location, and through diverse endpoint devices types.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. What are the benefits of application virtualization? Choose all that apply.

- a. Flexibility of application access
- b. Eliminate OS modifications
- c. Simplified OS image management
- d. Improved data protection and compliance

## Storage

Storage

## Storage

## Types of Storage

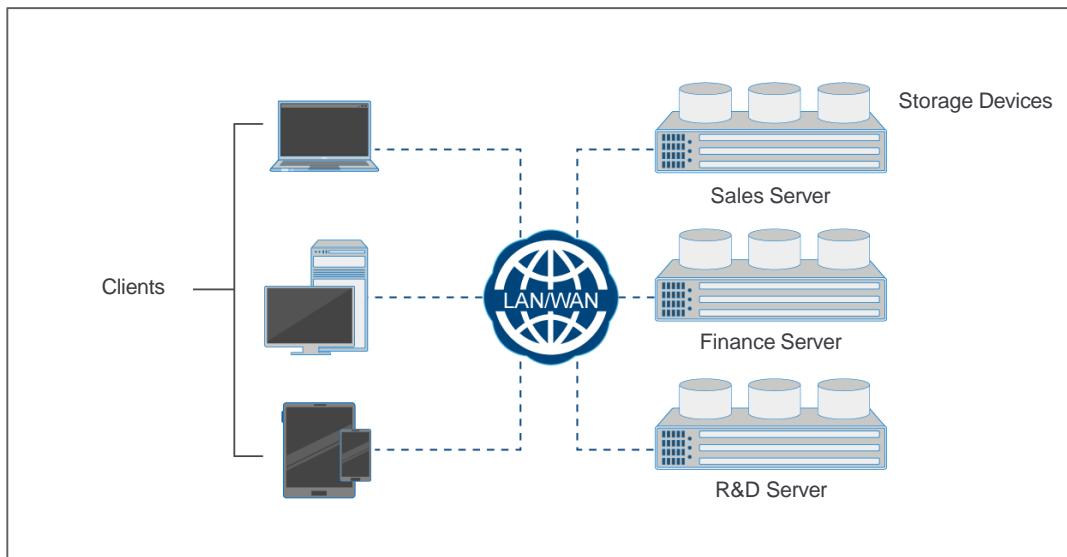
Storage Type	Description
<b>Magnetic Tape Drive</b>	<ul style="list-style-type: none"> <li>Stores data on a thin plastic film with a magnetic coating.</li> <li>Provides only sequential data access.</li> <li>Low-cost solution for long term data storage.</li> </ul>
<b>Hard Disk Drive (HDD)</b>	<ul style="list-style-type: none"> <li>Stores data on a circular disk with a ferromagnetic coating.</li> <li>Provides random read/write access.</li> <li>Most popular storage device with large storage capacity.</li> </ul>
<b>Solid State Drive (SSD)</b>	<ul style="list-style-type: none"> <li>Stores data on a semiconductor-based memory.</li> <li>Very low latency per I/O, low power requirements, and very high throughput.</li> <li>Architecture is much sturdier, so the data is not so vulnerable to loss or damage.</li> </ul>
<b>Non-Volatile Memory express (NVMe)</b>	<ul style="list-style-type: none"> <li>High-performance software interface for PCI express solid-state drives (SSDs) that use non-volatile memory (NVM).</li> <li>Takes advantage of the microsecond latency provided by all-flash arrays and eliminates the SCSI bottleneck.</li> <li>Offers greater storage throughput and lower latency.</li> </ul>

## Storage

<b>Storage Class Memory (SCM)</b>	<ul style="list-style-type: none"><li>• High-performance non-volatile storage that addresses the performance needs to support digital transformation.</li><li>• A new tier to the storage hierarchy, one that features memory-like performance at storage-like cost.</li><li>• Slower than DRAM but read and write speeds are over 10 times faster than flash and can support higher IOPS while offering comparable throughput.</li></ul>
<b>NVRAM</b>	<ul style="list-style-type: none"><li>• Subset of the larger category of non-volatile memory (NVM), which includes storage-class memory based on NAND flash.</li><li>• Used to store information about state of the components and devices in the computer for fast booting.</li></ul>

## Storage Architecture: DAS vs. SAN

### Server-centric Storage Architecture (Internal DAS)

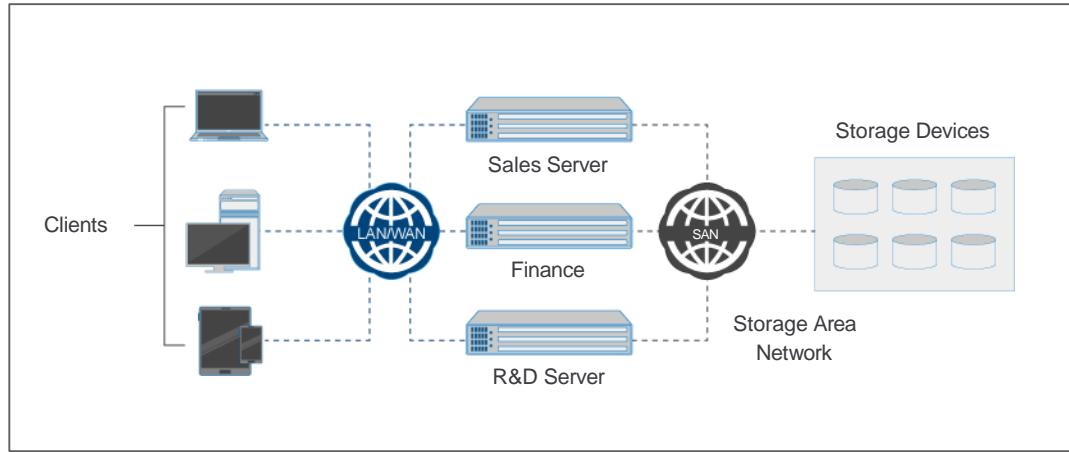


Server-centric storage architecture (click image to enlarge)

- Storage devices are connected directly to the servers and are typically internal to the server.
- Number of storage devices that can be connected to one server is limited, and it is not possible to scale the storage capacity.
- With HCI implementation, these internal storage devices can be shared among compute systems.

## Storage

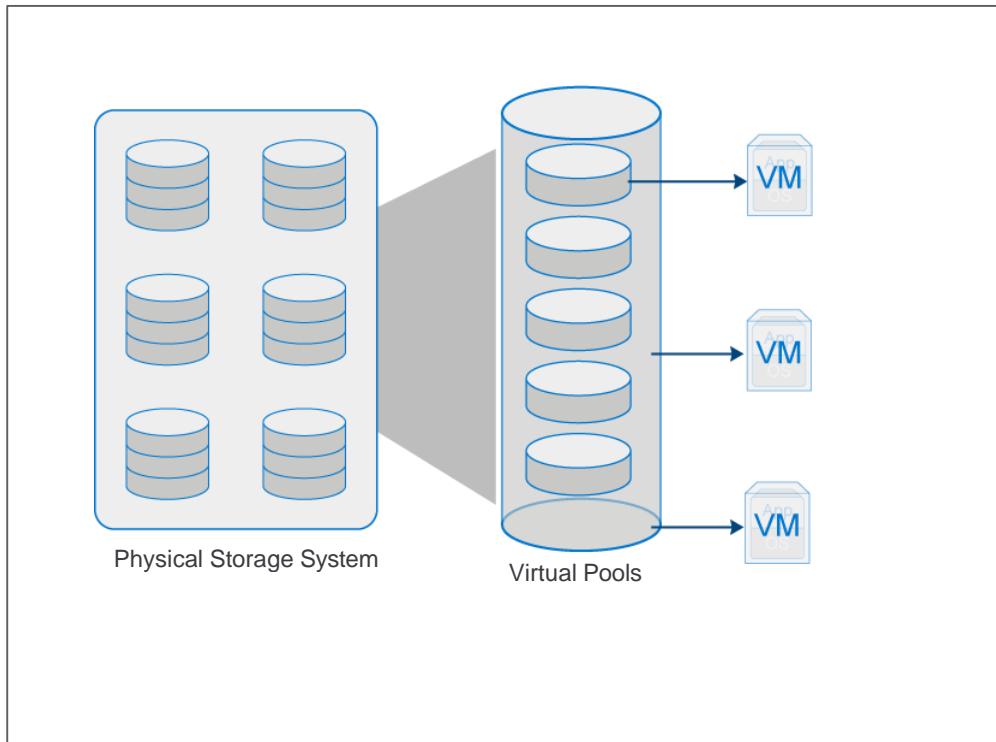
### Information-centric Storage Architecture (SAN)



*Information-centric storage architecture (click image to enlarge)*

- Storage devices exist independently of servers, and are managed centrally and shared between multiple compute systems.
- Storage capacity can be increased dynamically and without impacting information availability by adding storage devices to the pool.
- Improves the overall storage capacity utilization, while making management of information and storage more flexible and cost-effective.

## Storage Virtualization



- A technique of abstracting physical storage resources to create virtual storage resources.
- Storage virtualization software has the ability to pool and abstract physical storage resources, and present them as a logical storage resource, such as:
  - Virtual volumes
  - Virtual disk files
  - Virtual storage systems
- Software is either built into the operating environment of a storage system, installed on an independent compute system, or available as hypervisor's capability.

Knowledge Check

## Knowledge Check

## Knowledge Check

1. Which storage device uses high-performance software interface for PCI express solid-state drives (SSDs).
  - a. NVRAM
  - b. NVMe
  - c. SATA
  - d. SCM

Network

## Network

## Network

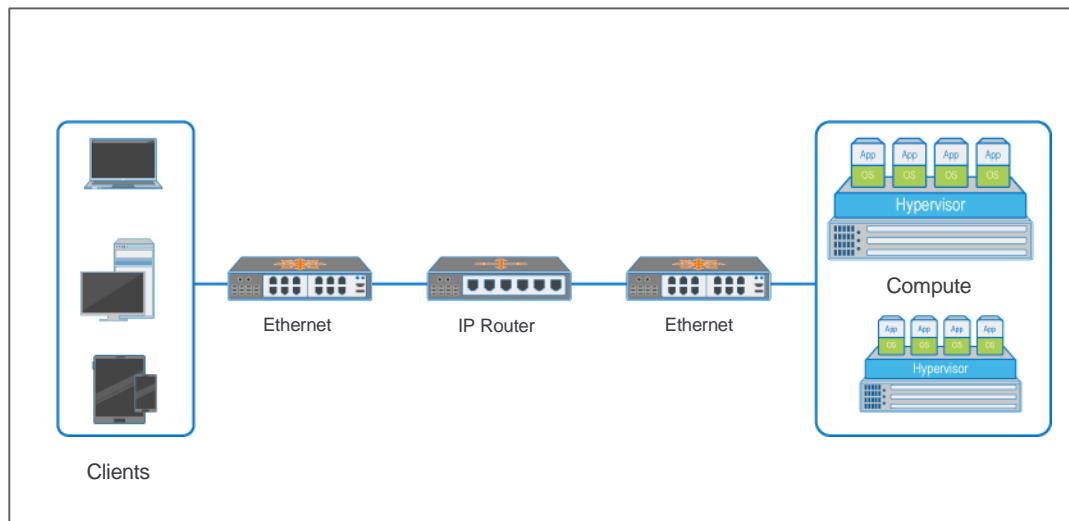
## Network Overview

Connectivity provides communication paths between IT infrastructure components for information exchange and resource sharing.

Organizations typically use different types of network supporting different network protocols, transport medium, and topology. The different types of network connectivity include:

***Click each tab to view details about the types of connectivity.***

### Compute-to-Compute Connectivity



*Interconnections between physical compute systems*

- Uses protocols based on the Internet Protocol (IP). Each physical compute system is connected to a network through one or more host interface devices,

called a network interface card (NIC). Physical switches<sup>26</sup> and routers<sup>27</sup> are the commonly used interconnecting devices.

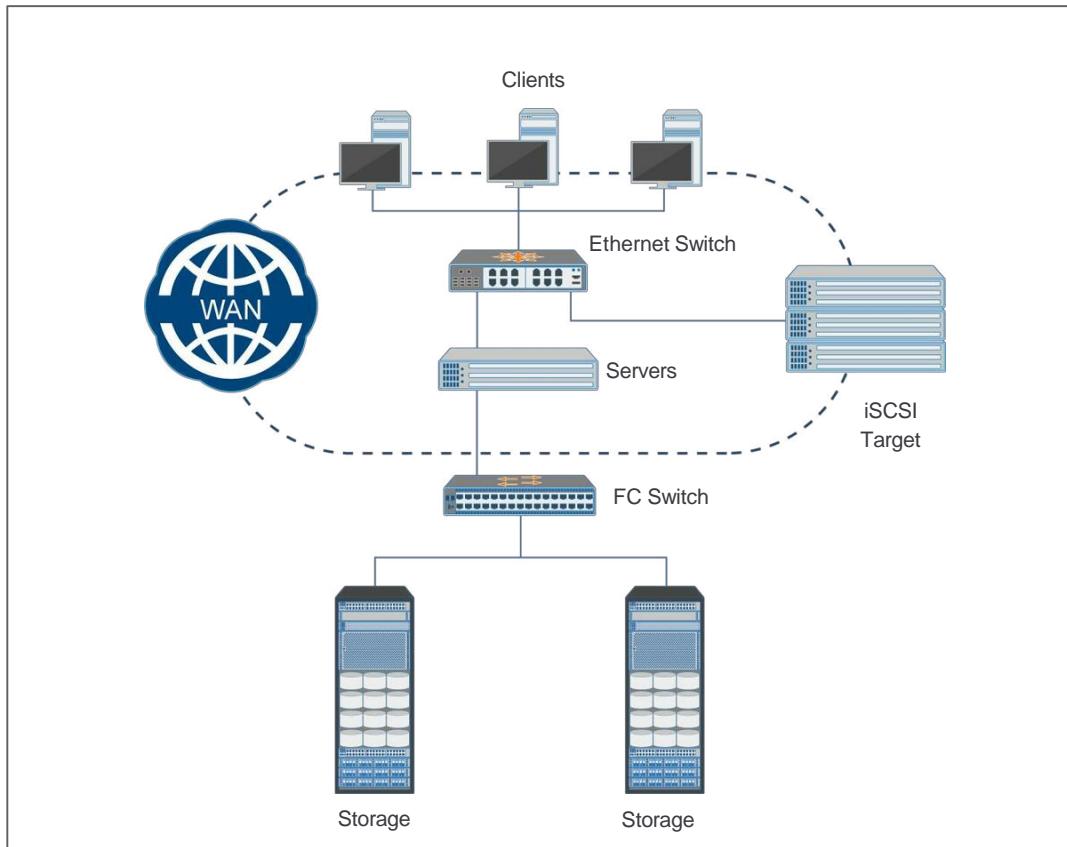
- The image shows a network (LAN or WAN) that provides interconnections among the physical compute systems. It is necessary to ensure that appropriate switches and routers, with adequate bandwidth and ports, are available to provide the required network performance.

---

<sup>26</sup> A switch enables different compute systems in the network to communicate with each other.

<sup>27</sup> A router is an OSI Layer-3 device that enables different networks to communicate with each other.

## Compute-to-Storage Connectivity

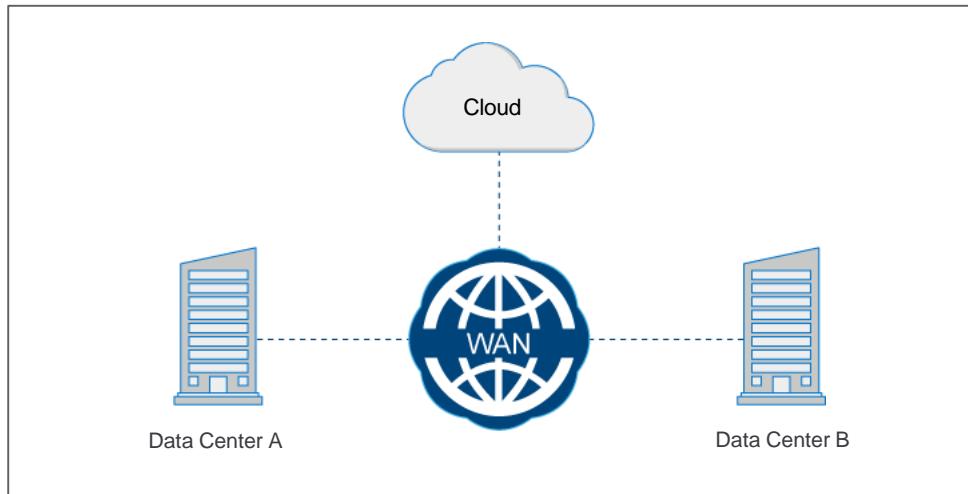


*Components connecting compute and storage systems*

- Storage may be connected directly to a compute system or over a SAN.

- Connectivity and communication between compute and storage are enabled through physical components and interface protocols.
- The physical components that connect compute to storage are: Host bus adapter<sup>28</sup>, port<sup>29</sup>, switches, and cable.

## Between Data Centers



*Multiple data centers connected through WAN*

---

<sup>28</sup> A host bus adapter (HBA) is a host interface device that connects a compute system to storage or to a SAN. It is an application-specific integrated circuit (ASIC) board. It performs I/O interface functions between a compute system and storage, relieving the processor from more I/O processing workload. A compute system typically contains multiple HBAs.

<sup>29</sup> A port is a specialized outlet that enables connectivity between the compute system and storage. An HBA may contain one or more ports to connect the compute system to the storage.

## Network

- The organizations may use IT resources at one or more data centers to provide IT services.
- Also, a data center may be inter-connected with multiple clouds to enable workload migration or distribution of workload across clouds.
  - Organizations can use Wide Area Network (WAN) to enable these services.

## Network Communication Protocols

- Digital communication networks rely on communications protocols to establish and maintain conversations between devices.
- A **protocol** is a set of functions based on a set of rules. All participants agree to use the same protocol to communicate.
- Protocols standardize how interconnected devices connect and communicate over a medium, such as wires or the air.
- Communications protocols are used to establish, maintain and terminate a conversation.
- Some popular protocols are:
  - Ethernet
  - TCP/IP
  - Fibre Channel (FC)
  - Fibre Channel over IP (FCIP)
  - Internet Small Computer System Interface (iSCSI)
  - NVMe over Fabrics

## The OSI Reference Model

Application	Application Interface to Lower Functions/Services
Presentation	Syntactic Data Representation (.JPG, .DOC, .PPT, etc.)
Session	Application Level Connection and Coordination
Transport	Logical End-to-End Connections / Sequencing, Integrity
Network	Logical Addressing and Routing
Data Link	Physical addressing, Framing Flow Control
Physical	Physical Media, Signal / Codes, Transmission

*The OSI reference model (click image to enlarge)*

The Open Systems Interconnection (OSI) reference model is a logical communications protocol for standardized network communication operation. It was developed by the International Standards Committee (ISO).

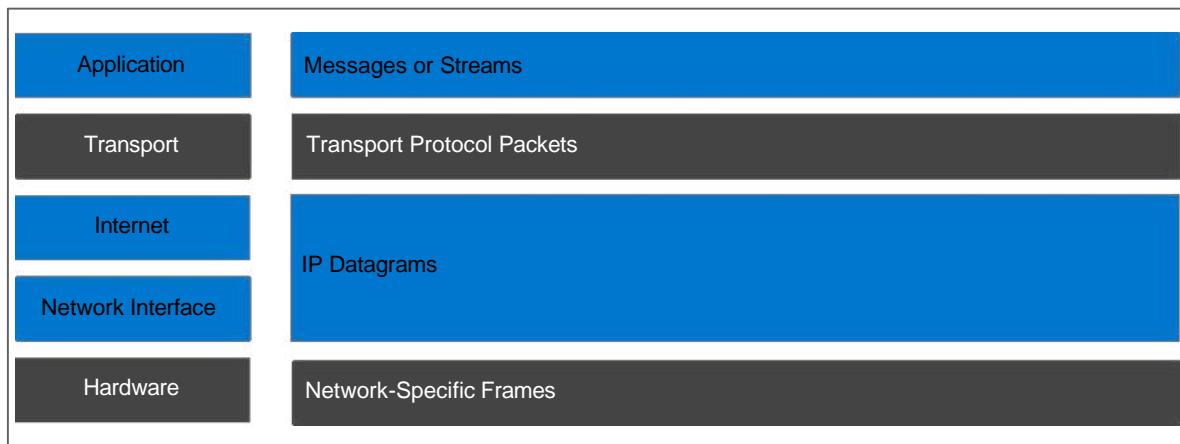
The protocol is described in seven layers, with each layer providing a part of the end-to-end networked interconnection and communication path.

- Each protocol layer is programmed to provide its function independently of the others.
  - Arranged in a protocol stack, each layer directly interfaces only with the layer immediately beneath and above.
- The output of each layer is accepted as input to the next until the communication exits the stack to the receiving device.
- Every end device must be running the same protocol stack in order to communicate with each other.
- Communicating devices must use the same protocol stack to establish and maintain a conversation.

## TCP/IP Reference Model

The TCP/IP protocol suite is expressed in 4 layers instead of 7 layers. The hardware layer is a placeholder for general network hardware and media functionality not included in TCP/IP layer programming.

- The TCP/IP model is named after its two primary protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP).
  - The TCP protocol controls data transmission and ensures data integrity. Message transmission order is maintained until delivery.
- The IP protocol handles the correct routing of messages across different networks, and interconnected devices.



*The TCP/IP model maps its protocol functionality across layers (click image to enlarge)*

## IP Addressing

The **Internet Protocol** works at layer 3, the Network layer of the OSI model and at the Internet layer of the TCP/IP model. A network device that uses IP addresses and makes the connection between end devices across different networks is called a **network router**.

- IP is an addressing scheme that enables end devices to connect across the same, or different networks.
- IP addresses are segmented into different sections that specify the network address, and the host address on that network.
  - IPv4 uses periods to separate sections.
  - A subnet mask specifies which sections of the IP address contain the network address or host address.
  - The segmented scheme is parsed by the router.
- The router establishes a logical path between devices on different networks.

### Notes:

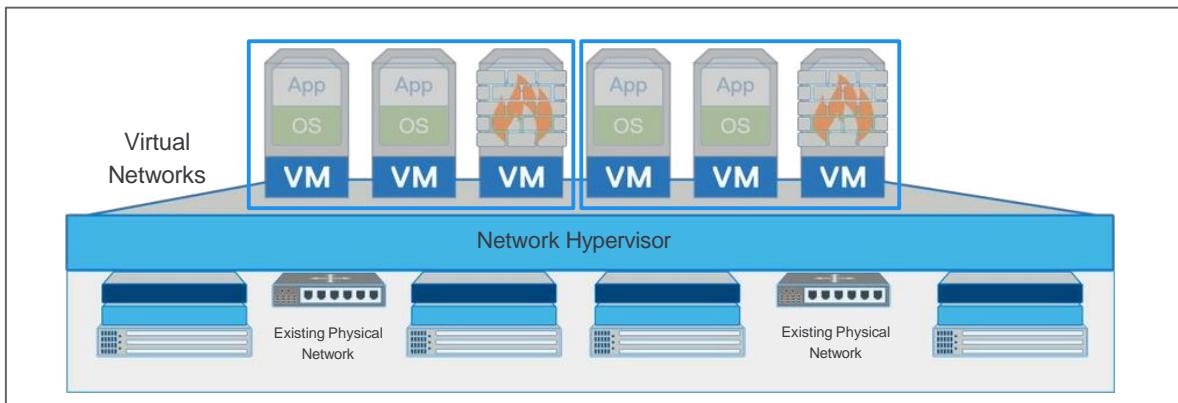
- An **IPv6 address** is a set of numbers divided by **colons** instead of periods. IPv6 addresses are much longer than IPv4 addresses, consisting of 128 bits in hexadecimal notation.
- IPv6 was developed to handle the exponentially increasing number of networked devices being connected over the worldwide Internet as the *Internet of Things* (IoT) evolves.
- Similar to IPv4 IP addresses, each section before a colon is a portion of the unique network address and device address.
- A subnet mask specifies which sections of the IPv6 address contain the network address, and which specifies the host address.
- IPv4 is typically used for local LAN connectivity, with IPv6 reserved for devices that connect over the Internet.

Here is an example of a typical IPv6 address:

**2002:ac18:af02:00f4:020e:cff:fe6e:d527**

## Network Virtualization

- Creates logical, virtual networks that are decoupled from the underlying network hardware to ensure the network can better integrate with and support increasingly virtual environments.
  - With virtualization, enterprises can take advantage of the efficiencies and agility of software-based compute and storage resources.
- Networks have been moving towards greater virtualization, it is only recently, with the true decoupling of the control and forwarding planes, as introduced by software-defined networking (SDN) that network virtualization has become a reality.



*Network virtualization*

Knowledge Check

## Knowledge Check

## Knowledge Check

1. What is the function of a host bus adapter?
  - a. Connects compute system to storage or SAN.
  - b. Connects storage server and FC switch.
  - c. Performs I/O interface functions between multiple storage systems only.
  - d. Performs I/O interface functions between multiple compute systems only.

## Knowledge Check

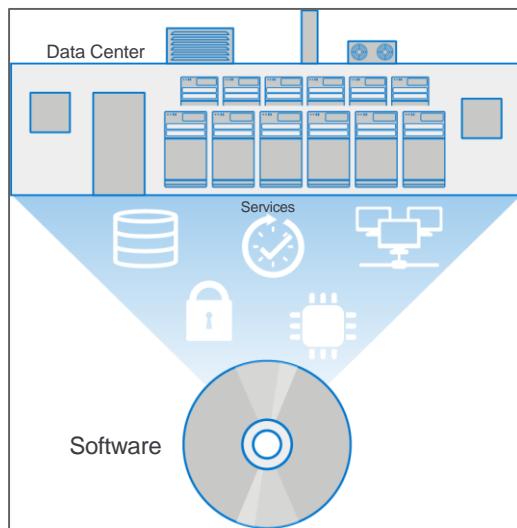
### Knowledge Check

2. What determines the portion of an IP address used to indicate the network or host address?
  - a. A subnet mask.
  - b. An octet.
  - c. A colon address field separation character.
  - d. A period address field separation character.

## Software-Defined Data Center (SDDC)

## Software-Defined Data Center (SDDC)

## Software-Defined Data Center (SDDC) Overview



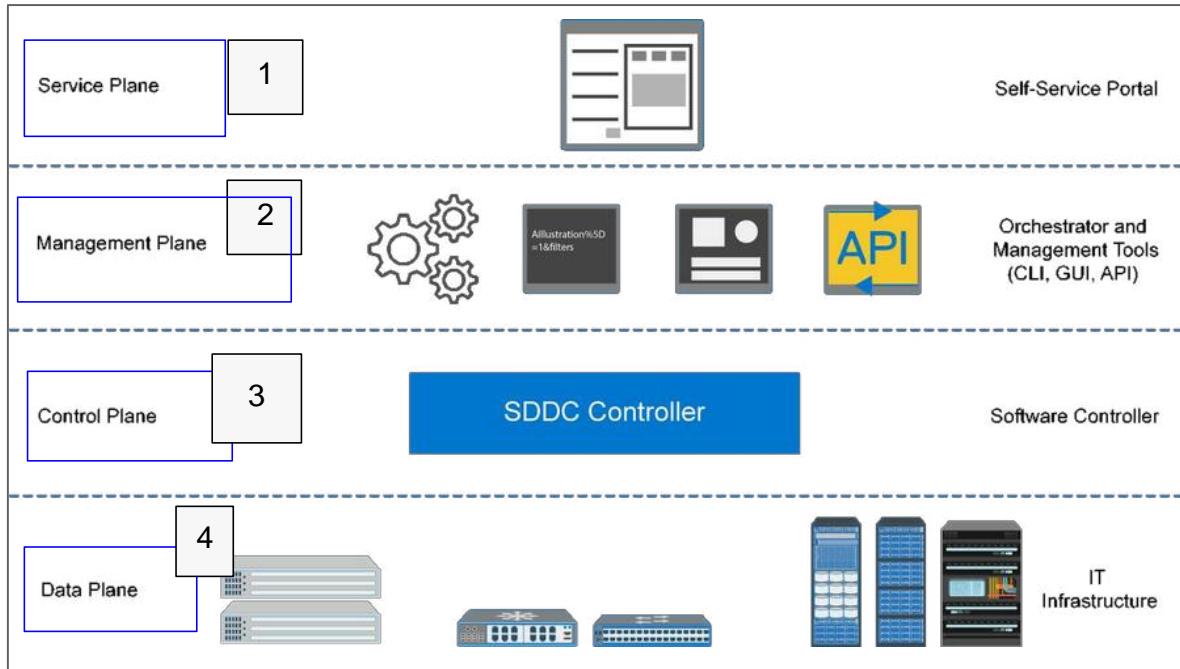
**SDDC** is an architectural approach to IT infrastructure that extends virtualization concepts such as abstraction, pooling, and automation to all of the data center's resources and services to achieve IT as a service.

## Software-Defined Data Center (SDDC)

### Software-Defined Data Center Architecture

Software-defined data center (SDDC) architecture includes four distinguished planes – data plane, control plane, management plane, and service plane.

**Click on the name of each plane on the image for more information.**



**1:** Allows a user to request or order a service from the catalog in a self-service way.

**2:** Used to perform administrative operations such as configuring a system and changing policies.

The management plane is responsible for communicating messages such as configuration, statistics, status, and real-time data between transport nodes and the management plane.

**3:** Provides the programming logic and policies that the data plane follows to perform its operations.

The key functions of the control plane include asset discovery, resource abstraction and pooling, provisioning resources for services.

**4:** Performs the data processing and I/O operations.

**Notes:**

- The SDDC architecture decouples the control plane from the data plane.
  - It separates the control functions from the underlying infrastructure components and provides it to an external software controller.
  - The centralized control plane provides policies for processing and transmission of data, which can be uniformly applied across the multi-vendor infrastructure components.
  - The policies can also be upgraded centrally to add new features and to address application requirements.
- The controller usually provides CLI and GUI for administrators to manage the IT infrastructure and configure the policies. It also automates and orchestrates many hardware-based or component-specific management operations.
  - This reduces the need for manual operations that are repetitive, error-prone, and time-consuming.
- The software controller provides APIs for external management tools and orchestrators to manage data center infrastructure and orchestrate controller operations.
- The SDDC architecture enables users to view and access IT resources as a service from a self-service portal.
  - The portal provides a service catalog that lists a standardized set of services available to the users.
- The service catalog allows a user to request or order a service from the catalog in a self-service way.
  - The request is forwarded to the software controller by an orchestrator or a management tool. Upon receiving the request, the controller provisions appropriate resources to deliver the service.

Knowledge Check

## Knowledge Check

## Knowledge Check

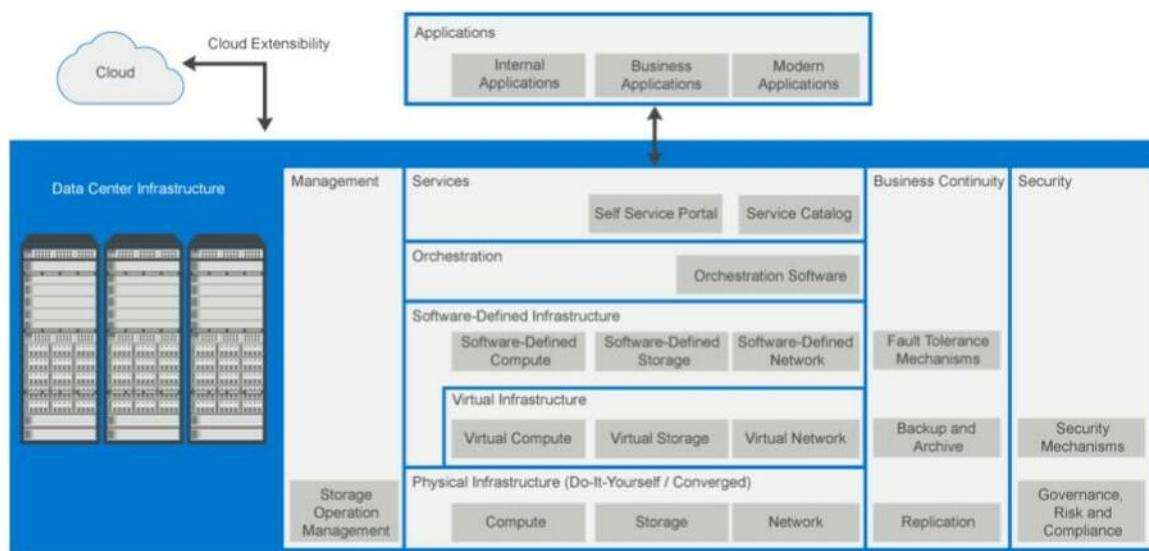
1. Which SDDC architecture plane performs administrative operations such as configuring a system and changing policies?
  - a. Management plane
  - b. Control plane
  - c. Data plane
  - d. Service plane

## Modern Data Center Architecture

## Modern Data Center Architecture

### Modern Data Center Architecture

- The IT infrastructure is arranged in five logical layers and three cross-layer functions.
  - The five layers are physical infrastructure, virtual infrastructure, software-defined infrastructure, orchestration, and services.
  - The three cross-layer functions are business continuity, security, and management.
- Ensures that the infrastructure can be transformed into a cloud infrastructure that could be either private or public.
- Further, by integrating cloud extensibility, the infrastructure can be connected to an external cloud to leverage the hybrid and multi-cloud model.



**1:** Applications that are deployed in the data center may be a combination of internal applications, business applications, and modern applications.

**2:** The management function includes various processes that enable the efficient administration of the data center and the services for meeting business requirements.

**3:** The physical infrastructure forms the foundation layer of a data center. It includes equipment such as compute systems, storage systems, and networking devices.

**4:** Virtualization is the process of abstracting physical resources, such as compute, storage, and network, and creating virtual resources from them.

Virtualization is achieved by using virtualization software that is deployed on compute systems, storage systems, and network devices.

**5:** The software-defined approach enables ITaaS, in which consumers provision all infrastructure components as services. It centralizes and automates the management and delivery of heterogeneous resources based on policies.

The key architectural components includes software-defined compute, software-defined storage (SDS), and software-defined network (SDN).

**6:** This layer provides workflows for executing automated tasks to perform a business operation.

The orchestration software enables this automated arrangement, coordination, and management of the tasks. This function helps to group and sequence tasks with dependencies among them into a single, automated workflow.

**7:** This layer includes a service catalog that presents the information about all the IT resources being offered as services.

The service catalog is a database of information about the services and includes various information about the services, including the description of the services, the types of services, cost, supported SLAs, and security mechanisms.

**8:** The business continuity (BC) cross-layer function specifies the adoption of proactive and reactive measures that enable an organization to mitigate the impact of downtime due to planned and unplanned outages.

**9:** The security cross-layer function supports all the infrastructure layers—Physical, Virtual, Software-defined, Orchestration, and Services.

Provide secure services to the consumers. Security specifies the adoption of administrative and technical mechanisms that mitigate or minimize the security threats and provide a secure data center environment.

Knowledge Check

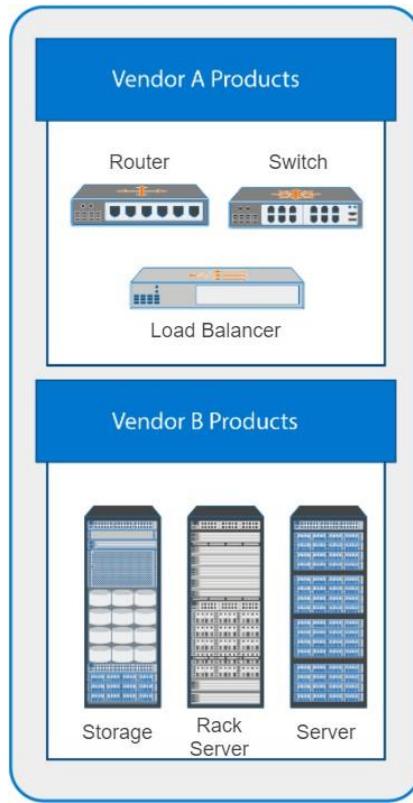
## Knowledge Check

## Knowledge Check

1. Which data center architecture layer provides workflows for executing automated tasks to accomplish business outcomes?
  - a. *Orchestration*
  - b. Security
  - c. Services
  - d. Management

## Building a Modern Data Center

## Do-It-Yourself Approach



In the Do-It-Yourself (DIY) approach, organizations integrate the best in class infrastructure components including hardware and software that is purchased from different vendors. This approach:

- Utilizes products and services from the respective leading vendors and provides specific functions with more configuration options.
- Requires integration and testing for compatibility between the various components and the existing infrastructure.
- Enables organizations to select vendors of their choice for infrastructure components.
- Provides an option for organizations to switch vendors if they are unable to provide the required performance or service levels.

## DIY Methods

You can build the infrastructure for modern data center in two methods using the do-it-yourself approach.

### Greenfield

**Greenfield Method:** Greenfield environments enable architects to design exactly what is required to meet the business needs using new infrastructure that is built specifically for a purpose. Greenfield environments can avoid some of the older and less efficient processes, rules, methods, misconfigurations, constraints, and bottlenecks that exist in the current environment. Greenfield environments also have the added benefit of enabling a business to migrate infrastructure to a different technology or vendor and to build in technologies that help avoid future lock-in. But greenfield environments also have some downsides, such as higher cost, lack of staff expertise, and possibly increased implementation time.

### Brownfield

**Brownfield Method:** This method involves upgrading or adding new infrastructure elements to the already existing infrastructure. This method allows organizations to repurpose the existing infrastructure components, providing a cost benefit. Simultaneously the organization may face integration issues, which can compromise the stability of the overall system. Existing infrastructure or processes such as resource type, available capacity, provisioning processes and managing the resources may place extra constraints on the architect's design. These constraints may negatively affect performance or functionality.

## Vendor Ready Solutions



Today, IT is looking for ways to reduce deployment time, management complexity and automate the resource provisioning processes. Therefore, organizations are adopting pre-integrated systems to bring together compute, network, storage, virtualization, and management technologies, and delivered them as one engineered system.

- These pre-integrated systems are developing at a rapid pace and are suitable for the data centers of all sizes.
- Compared to DIY approach, the vendor ready solutions integrates high-quality hardware and software components that make up a data center into a single packaged solution.
  - In this case, the flexibility of choice is limited although some vendors provide options to choose among multivendor IT components.
- Typically, the vendor ready solution has a single management software capable of managing all hardware and software within the package.
  - With DIY approach, organizations usually deploy multiple management tools to manage multivendor IT infrastructure components.

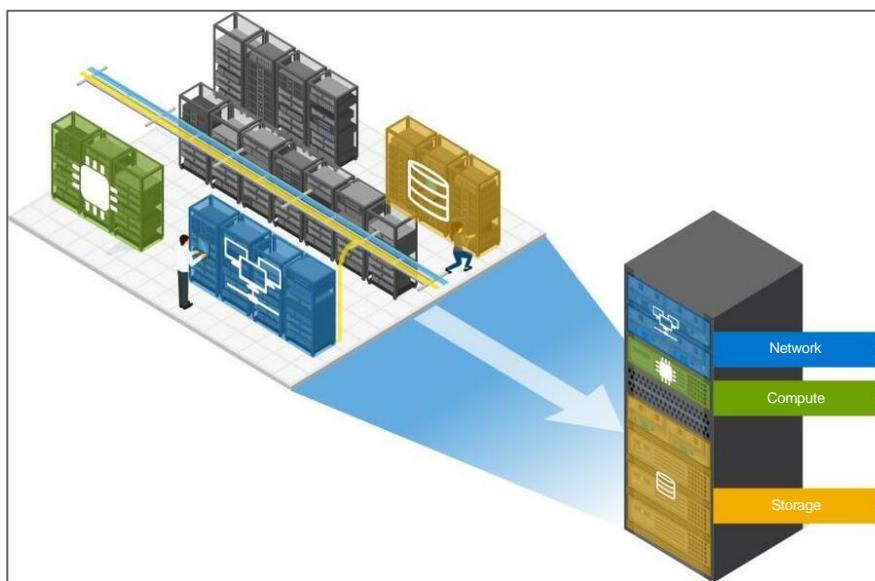
Converged and Hyper-converged infrastructure can help to simplify either the DIY or vendor ready solutions approach.

## Converged and Hyper-Converged Infrastructure

There are two types of converged systems:

***Click each tab to view details about CI/HCI infrastructure.***

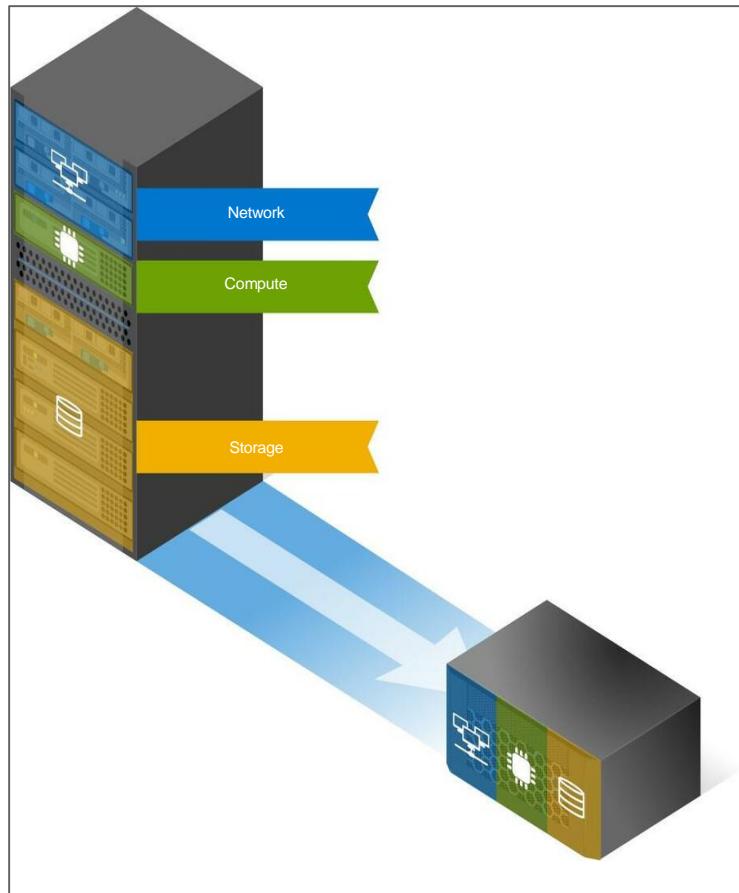
### Converged Infrastructure (CI)



IT components that make up a data center can be packaged into a single, standalone computing box, called converged infrastructure.

- The package is a self-contained unit that can be deployed independently, or aggregated with other packages to meet additional capacity and performance requirements.
- Components of a converged infrastructure may include compute systems, data storage devices, networking equipment, and software for IT infrastructure management, data protection, and automation.

## Hyper-converged Infrastructure (HCI)



Hyperconverged Infrastructure (HCI) combines the datacenter components of compute, storage, virtualization, and storage networking into a distributed infrastructure platform, managed by software.

- The intelligent HCI software can create flexible building blocks called nodes, thereby replacing legacy infrastructure, including separate servers, and storage networks and arrays.
- Unlike Converged Infrastructure (CI), which relies on hardware and uses physical building blocks, HCI is software-defined. Moreover, HCI is more flexible and scalable than CI.

## Data Center as a Service (DCaaS)



- Clients can rent or lease access to the provider's data center, using the servers, networking, storage and other computing resources owned by the DCaaS provider.
- Empowers your entire organization to focus on business innovation and differentiation. Through DCaaS solution:
  - **IT Operations** can offload maintenance and refocus on value-added services.
  - **IT Architects** can offload everything including initial deployment, patching and upgrades of the software, hardware and monitoring to simplify operations.
  - **IT Security** can uniformly apply security policies, eliminating the need to track and secure workloads that span multiple environments.
  - **IT decision makers** can negotiate one contract with one vendor for all core and edge data center needs.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Which of the following statement is correct about converged and hyperconverged infrastructure? Choose all that apply.
  - a. *CI is a self-contained unit that can be deployed independently, or aggregated with other packages to meet additional capacity and performance requirements.*
  - b. *Hyperconverged infrastructure (HCI) combines the datacenter components of compute, storage, virtualization, and storage networking into a distributed infrastructure platform, managed by software.*
  - c. Converged infrastructure is a software-defined infrastructure which is more flexible and scalable than hyperconverged infrastructure.
  - d. IT components that make up a data center can be packaged into a single, standalone computing box, called hyperconverged infrastructure.

## Concepts in Practice

## Concepts in Practice

### Dell EMC PowerEdge Server

The new PowerEdge server portfolio is built to power your innovation engine to meet the challenges of digital transformation with a secure infrastructure that supports a full range of modern workloads and objectives.

- The PowerEdge Server family includes various types of servers that include Tower servers, Rack servers, and Modular Servers.
- PowerEdge servers deliver the productivity and performance you need to power your innovation.
- The scalable business architecture of PowerEdge helps you provide optimized performance for a multitude of workloads.
- Use OpenManage to eliminate or automate routine management and free up skilled resources.
- Integrated security from PowerEdge protects one of the most important assets of your company – your infrastructure.



### Dell EMC VxBlock

The VxBlock System 1000 is a converged infrastructure solution.

- Combines compute, virtualization, network, storage, management, and data protection components into a single package.
- Supports traditional and modern workloads, including data analytics, big data, mission-critical enterprise applications, and more.

- Combines industry-leading technologies that include Dell EMC storage and data protection options, Cisco UCS blade and rack servers, Cisco LAN and SAN networking, and VMware virtualization and cloud management into one fully integrated system.
- Leverages its deep VMware integration to simplify automation of everything from daily infrastructure provisioning tasks to delivery of IaaS and SaaS.



## Dell EMC VxRail

VxRail is a fully integrated, preconfigured, and tested Hyper Converged Infrastructure (HCI) system optimized for VMware vSAN and is the standard for transforming VMware environments.

## Concepts in Practice

- Provides a simple, cost effective hyperconverged solution that solves a wide range of your operational and environmental challenges and supports almost any use case, including tier-one applications, cloud native and mixed workloads.
- VxRail HCI system software, a suite of integrated software elements that sits between infrastructure components such as vSAN and VMware Cloud Foundation, delivers a seamless and automated operational experience.



## Dell EMC PowerFlex

Dell EMC PowerFlex is a hyperconverged solution that delivers flexible, scalable, and highly-performant software-defined storage.

- PowerFlex is designed for mission-critical, SLA-sensitive workloads by delivering extreme performance, massive scalability, and 99.9999% availability.
- Provides unprecedented architectural freedom to support heterogeneous workloads ranging from bare-metal and virtualized, to modern containerized.
- Enables organizations to achieve consistent outcomes for their most demanding workloads, with extensive automation and a broad ecosystem of validated enterprise workloads.



## Dell EMC Ready Stack: VMware vSphere with PowerStore Storage

Dell EMC Ready Stack solutions are proven, tested, and optimized to help organizations meet long-term data center needs for various mixed workloads. This

Ready Stack solution provides the simplicity of a complete, yet flexible, validated converged infrastructure (CI).

PowerStore storage achieves new levels of agility and operational versatility for today's cloud-mobile IT infrastructure. Using a containerized software architecture, the PowerStore system:

- Incorporates the best modern storage technology and eliminates the typical tradeoffs in performance, scalability, and storage efficiency.
- Provides advanced services to complement and extend existing on-premises environments.
- Supports an enterprise-class variety of traditional and modern workloads, relational databases, ERP and Electronic Medical Record (EMR) apps, cloud native applications, and file-based workloads such as content repositories and home directories.
- Appliances built on a container-based software architecture, known as PowerStoreOS, that provides unique capabilities for delivering and integrating advanced system services.
- Streamlines application development and automates storage workflows through integration with a broad ecosystem of leading DevOps and open management frameworks.

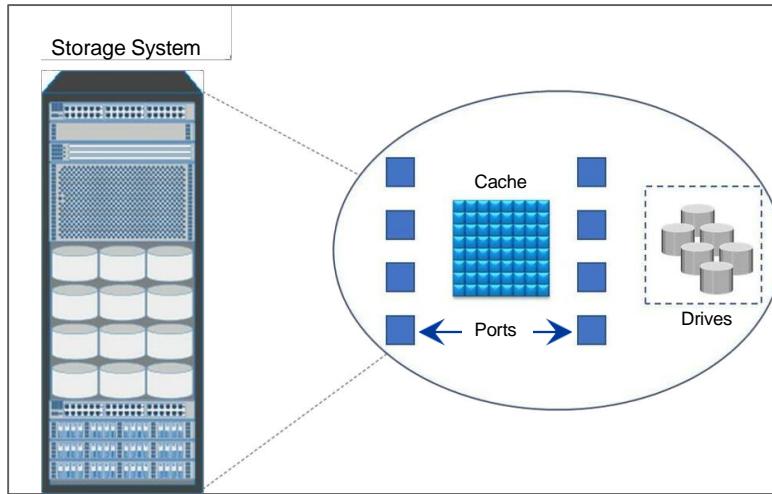


# Intelligent Storage System

## Intelligent Storage Systems

## Intelligent Storage System (ISS) Overview

## Intelligent Storage System (ISS) Overview

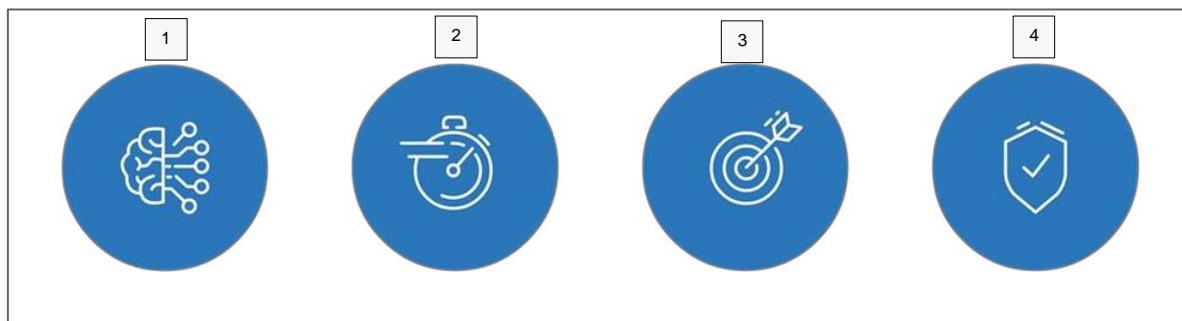


- An Intelligent storage system (ISS) is a feature-rich storage array that provides highly optimized I/O processing capabilities.
  - It has a purpose-built operating environment that intelligently and optimally handles the management, provisioning, and utilization of storage resources.
- Configured with a large amount of cache memory and multiple I/O paths to meet the requirements of performance-intensive applications.
- ISS ensures integrity of data, while addressing challenges around privacy and compliance.

### Key Features of an Intelligent Storage System

An intelligent storage system is designed for performance, scalability, and availability. Storage systems are fast, smart, efficient, and trusted providing the best solution for modern data centers.

Smart	Fast	Efficient	Trusted
<i>ISS uses Machine Learning to optimize performance and reduce cost.</i>	<i>ISS delivers unprecedented levels of performance.</i>	<i>Scale-up and scale-out architecture allows you to start small and grow as the business demands.</i>	<i>With ISS, data is always protected and available.</i>



**1:** Leverage integrated machine learning, always-on availability, multicloud integration, deduplication, compression, and encryption. Manual processes like initial volume placement, migrations, load balancing, and issue resolution are automated by machine learning (ML) engine, which optimizes performance and reduces cost. ISS uses a variety of AI/ML techniques to learn from workload themselves. AI/ML optimizes data placement between NVMe Flash and SCM drives. It automatically recognizes I/O profiles and move data in real time to the appropriate media types.

**2:** Non-Volatile Memory Express, or NVMe, is a high-performance protocol that is designed for modern media. NVMe-based flash drives used in intelligent storage systems take advantage of the parallelism of modern CPUs and SSDs, overcoming

performance limitations of spinning disk drives. Accelerate performance with end-to-end NVMe, multi-controller, scale-out, and SCM persistent storage.

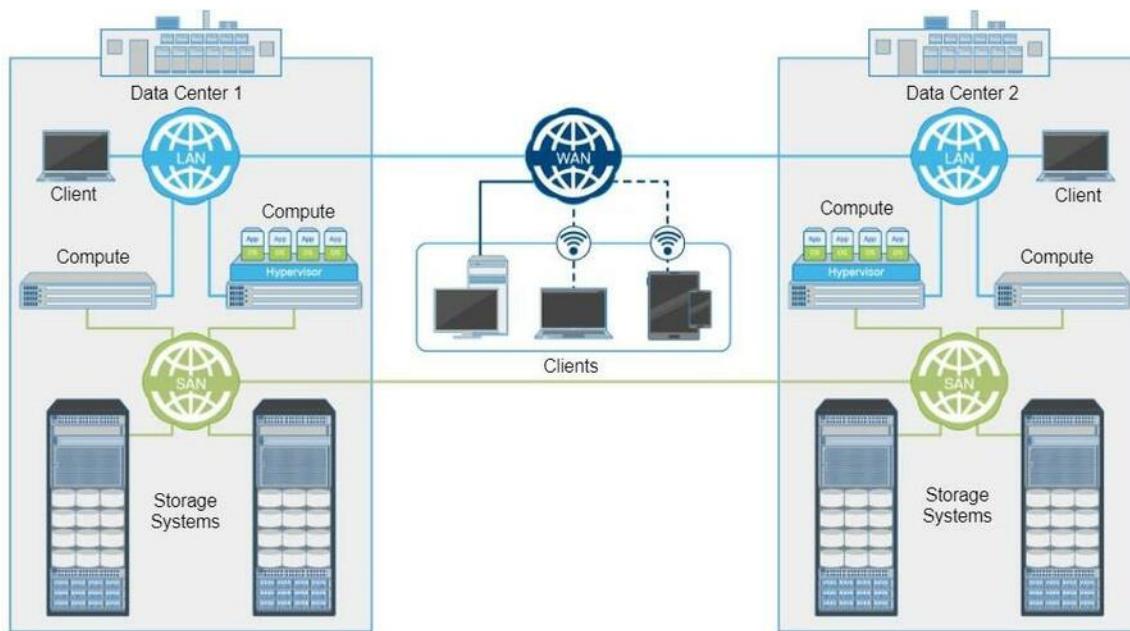
**3:** Intelligent storage systems consist of controllers and storage capacity. These components can be scaled-up and scaled-out by adding capacity. Data reduction, using compression and deduplication, provides significant consolidation, saving space and capacity.

**4:** Intelligent storage systems provide trusted solutions with rich data services such as data protection, Data at Rest Encryption (D@RE), and data reduction. It also provides the features such as non-disruptive upgrades, and migrations. Replication and backup provide data recovery when there is a disaster. D@RE protects confidentiality by encrypting all drives on the storage system. This encryption ensures protection from unauthorized access if drives are removed from the system.

### Intelligent Storage System Types

Based on the supported level of data access, primary storage systems can be classified as:

#### SAN Storage (Block-based)

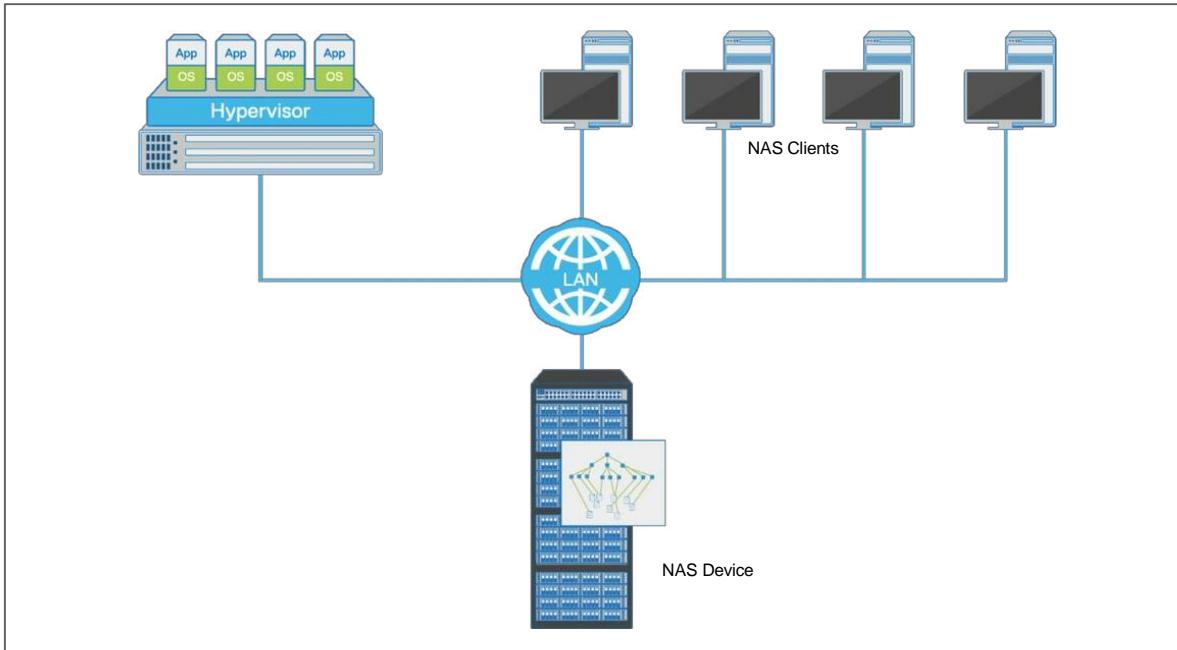


*SAN Storage Implementation*

A Storage Area Network (SAN) storage is a block-based storage system.

- SAN connects block-based storage with each other and to the compute systems.
- SAN storage improves the utilization of storage resources compared to a direct-attached storage (DAS) environment.
- With long-distance SAN, data transfer between SAN-attached storage systems can be extended across geographic locations.

### Network-Attached Storage (NAS)

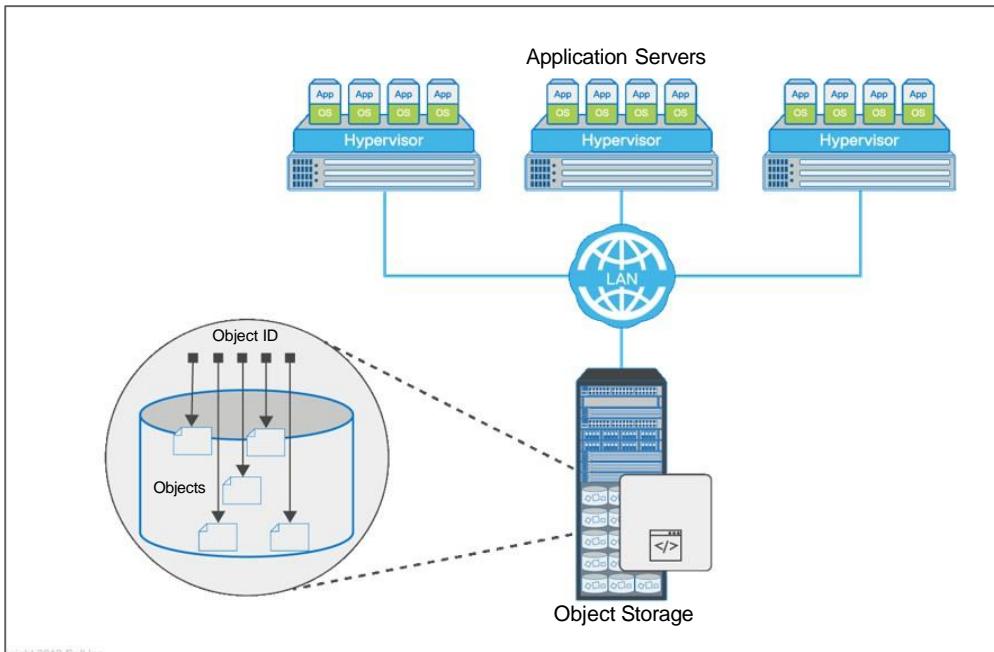


NAS is a dedicated, high-performance file sharing and storage device.

- Administrators create file systems on NAS systems, create shares, and export shares to NAS clients.
- NAS enables both Linux and Microsoft Windows users to share the same data.
  - It uses file-sharing protocols such as CIFS/SMB and NFS to provide access to the file data.

## Intelligent Storage System (ISS) Overview

### Object-Based Storage Device (OSD)



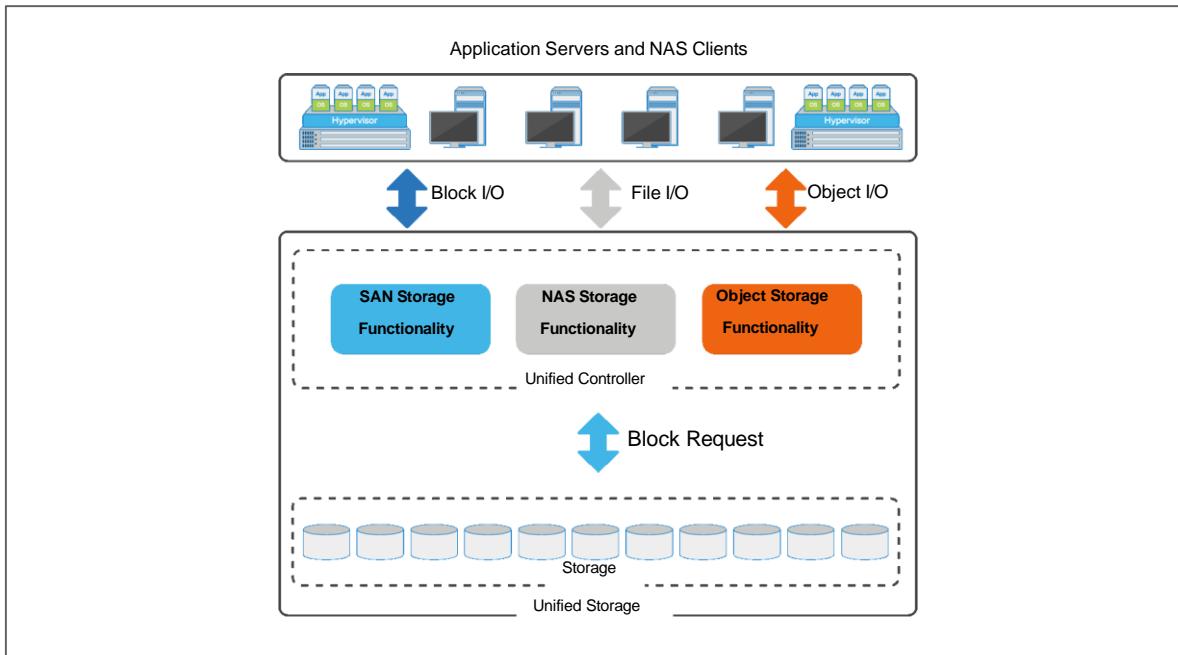
OSD stores data in the form of objects on a flat address space. All objects exist at the same level, and an object cannot be placed inside another object.

- An Object that is stored in an OSD is identified by a unique identifier called an object ID<sup>30</sup>.

---

<sup>30</sup> The object ID allows easy access to objects without the need to specify their storage locations.

## Unified Storage



Unified storage is a single storage system that consolidates block-level, file-level, and object-level access and is managed centrally.

- In some implementations, there are dedicated or separate controllers for handling block I/O, file I/O, and object I/O.
- The sharing of the storage resources increases storage utilization.

## ISS Types: Additional Information



*To understand the various types of ISS, click [here](#).*

## Knowledge Check

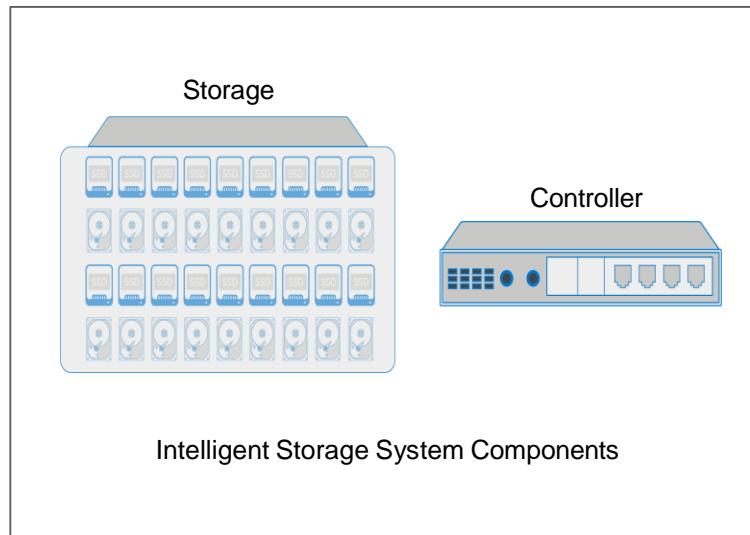
## Knowledge Check

1. Which is a SAN storage system?
  - a. NAS-based storage system
  - b. Block-based storage system
  - c. File-based storage system
  - d. Object-based storage system

## Intelligent Storage System Components

## Intelligent Storage System Components

## Intelligent Storage System Components



## Intelligent Storage System Components

- An intelligent storage system has two key components.
  - Controller<sup>31</sup> is a compute system that runs a purpose-built operating system that is responsible for performing several key functions for the storage system.
    - Serving I/O operations from the application servers.
    - Storage management.
    - RAID protection.
    - Local and remote replication.
    - Automated storage tiering, deduplication, data compression, data encryption, and intelligent cache management.
  - Storage
    - A storage system can have: hard disk drives (HDD), solid state drives (SSD), NVMe drives, and Storage Class Memory (SCM).

---

<sup>31</sup> An intelligent storage system typically has more than one controller for redundancy. Each controller consists of one or more processors and a certain amount of cache memory to process many I/O requests. These controllers are connected to the compute system either directly or through a storage network. The controllers receive I/O requests from the compute systems that are read or written from or to the storage by the controller.

## Hard Disk Drive



*To view the video about hard disk drive components, click [here](#).*

A hard disk drive is a persistent storage device that stores and retrieves data using rapidly rotating disks (platters) coated with magnetic material.

### Notes:

I/O operations in hard drives are performed by rapidly moving the arm across the rotating flat platters that are coated with magnetic material.

Data is transferred between the disk controller and magnetic platters through the read/write (R/W) head which is attached to the arm. Data can be recorded and erased on magnetic platters any number of times.

A typical hard disk drive consists of one or more flat circular disks called **platters**. The data is recorded on these platters in binary codes. The set of rotating platters is sealed in a case, called Head Disk Assembly (HDA). A platter is a rigid, round disk coated with magnetic material on both surfaces (top and bottom). The data is encoded by polarizing the magnetic area or domains of the disk surface. Data can be written to or read from both surfaces of the platter. The number of platters and the storage capacity of each platter determine the total capacity of the drive.

A **spindle** connects all the platters and is connected to a motor. The motor of the spindle rotates with a constant speed. The disk platter spins at a speed of several thousands of revolutions per minute (RPM).

**Read/write (R/W) heads**, read and write data from or to the platters. During reads and writes, the R/W head senses the magnetic polarization and never touches the surface of the platter. When the spindle rotates, a microscopic air gap is maintained between the R/W heads and the platters, which are known as the head flying height. This air gap is removed when the spindle stops rotating and the R/W head

## Intelligent Storage System Components

rests on a special area on the platter near the spindle. This area is called the landing zone.

R/W heads are mounted on the **actuator arm assembly**, which positions the R/W head at the location on the platter where the data must be written or read. The R/W heads for all platters on a drive are attached to one actuator arm assembly and move across the platters simultaneously.

The **controller** is a printed circuit board, mounted at the bottom of a disk drive. It consists of a microprocessor, internal memory, circuitry, and firmware. The firmware controls the power that is supplied to the spindle motor and controls the speed of the motor. It also manages the communication between the drive and the compute system. In addition, it controls the R/W operations by moving the actuator arm and switching between different R/W heads, and performs the optimization of data access.

## Hard Disk Drive Performance

A disk drive is an electromechanical device that governs the overall performance of the storage system environment.



*To understand about seek time and rotational latency, click [here](#).*

The various factors that affect the performance of disk drives are:

- Seek time<sup>32</sup>
  - Rotational latency<sup>33</sup>
  - Data transfer rate<sup>34</sup>
- 

<sup>32</sup> The seek time (also called access time) describes the time that is taken to position the R/W heads across the platter with a radial movement. In other words, it is the time that is taken to position and settle the arm and the head over the correct track. The lower the seek time, the faster the I/O operation.

<sup>33</sup> To access data, the actuator arm moves the R/W head over the platter to a particular track while the platter spins to position the requested sector under the R/W head. The time taken by the platter to rotate and position the data under the R/W head is called rotational latency. This latency depends on the rotation speed of the spindle and is measured in milliseconds.

**Disk service time = Seek time + Rotational latency + Data transfer rate**



**Caution:** The utilization of a disk I/O controller has a significant impact on the I/O response time. If the controller is busy or heavily used, that is, as the I/O controller saturates, the response time moves closer to infinity. The saturated component forces the serialization of I/O requests. Each I/O request must wait for the completion of the I/O requests that preceded it.

---

<sup>34</sup> The data transfer rate (also called transfer rate) denotes the average amount of data per unit time that the drive can deliver to the HBA. In a read operation, the data first moves from disk platters to R/W heads; then it moves to the drive's internal buffer. Finally, data moves from the buffer through the interface to the HBA on a compute.

## Why Flash Storage?

Most organizations that have achieved IT transformation are using flash storage.  
The benefits include:

### Faster Performance



Organizations using flash storage collectively report a 36% average increase in speeds, and a 49% improvement in application performance.

### Lower OpEx Expenses



Organizations using flash storage report a 42% reduction in operational costs. With no moving parts, minimal heat output and increased performance density, flash enables organizations to reduce power and cooling costs. It also eliminates maintaining large volume of HDDs and the associated costs for people, storage footprints, and cooling.

### Higher Throughput



Prior to flash, storage represented the slowest part of the data path and hosts and networks were inevitably waiting for storage to respond to I/O requests. With flash, servers can process thousands of transactions per second and systems are no longer in a perpetual “wait state.”

### Reduced CapEx Costs



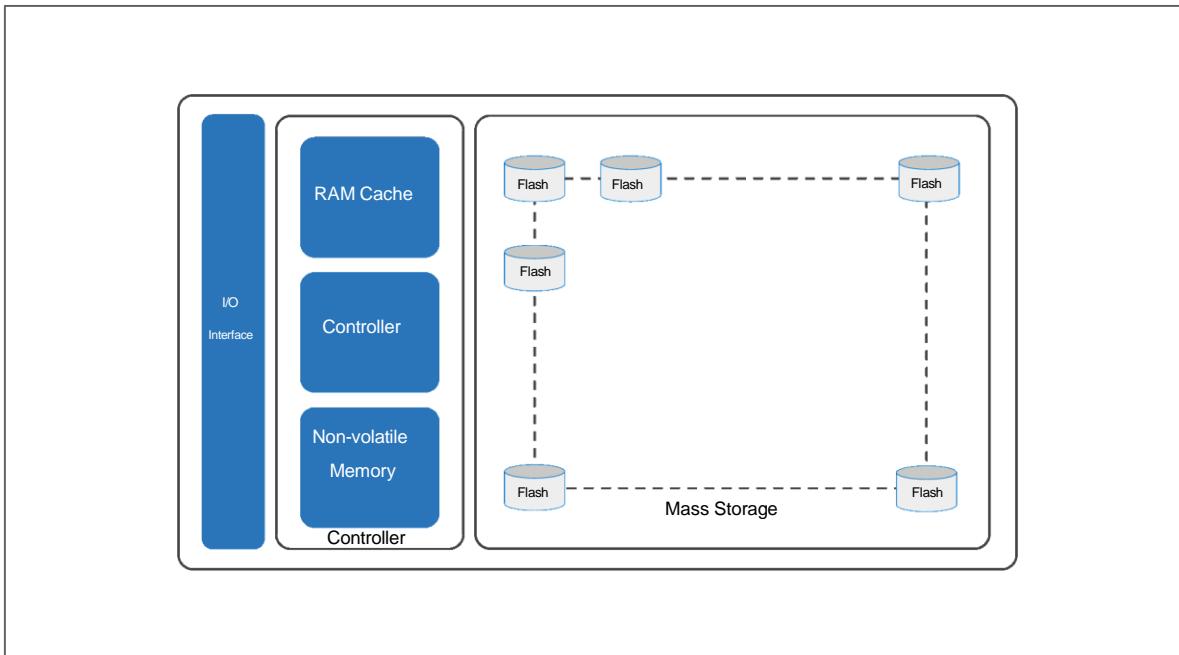
The cost of flash storage (per TB/GB) is declining and hence organizations' flash storage proportions are on the rise. The use of flash drives can reduce CAPEX of storage infrastructure.

### Faster decision-making



While big data analytics platforms can produce near real-time business intelligence, they require a level of performance that HDD storage system and cloud storage cannot always deliver. Analytics queries made to flash-supported workloads with structured or unstructured data get responses more quickly. This approach enables organizations to make better, faster, data-driven decisions than their competitors.

### Solid State Drive



*SSD internal architecture*

Solid state drives (SSDs) are data storage devices that use non-volatile flash storage to store data persistently. SSDs emulate conventional hard drives and are available with the same interfaces that hard drives use. SSDs consume less power compared to hard disk drives. Because SSDs do not have moving parts, they generate less heat compared to HDDs.

- Internally, the hardware architecture of a SSD consists of the following components:

- I/O interface<sup>35</sup>
  - Controller<sup>36</sup>
  - Mass storage<sup>37</sup>
- 

<sup>35</sup> The I/O interface connects the power and data connectors to the SSDs. Some of the interface protocols used to connect SSDs into compute system and storage infrastructure are Serial Attached SCSI (SAS), Serial ATA (SATA), and PCI-Express.

<sup>36</sup> The controller includes a drive controller, RAM, and non-volatile memory (NVRAM). The drive controller manages all drive functions. The non-volatile RAM (NVRAM) is used to store the SSD's operational software and data. Not all SSDs have separate NVRAM. Some models store their programs and data to the drive's mass storage. The RAM is used in the management of data being read and written from the SSD as a cache, and for the SSD's operational programs and data. SSDs include many features such as encryption and write coalescing.

<sup>37</sup> The mass storage is an array of nonvolatile memory chips. It retains the contents when powered off. These chips are commonly called Flash memory. The number and capacity of the individual chips vary directly in relationship to the SSD's capacity. The larger the capacity of the SSD, the larger is the capacity and the greater the number of the flash memory chips.

### Solid State Drive Performance



- SSDs perform better random reads.
- SSDs use all internal I/O channels in parallel for multithreaded large block I/O operations.
- SSDs are best for workloads with short bursts of I/O activity.

#### Notes:

SSDs are semiconductor, random-access devices. These result in low response times compared to hard disk drives. SSD performance is dependent on access type, drive state, and workload duration. SSD performs random reads the best.

In carefully tuned multi-threaded, small-block random I/O workload storage environments, SSDs can deliver much shorter response times and higher throughput than hard drives. Because they are random access devices, SSDs pay no penalty for retrieving I/O that is stored in more than one area; as a result their response time is in an order of magnitude faster than the response time of hard drives.

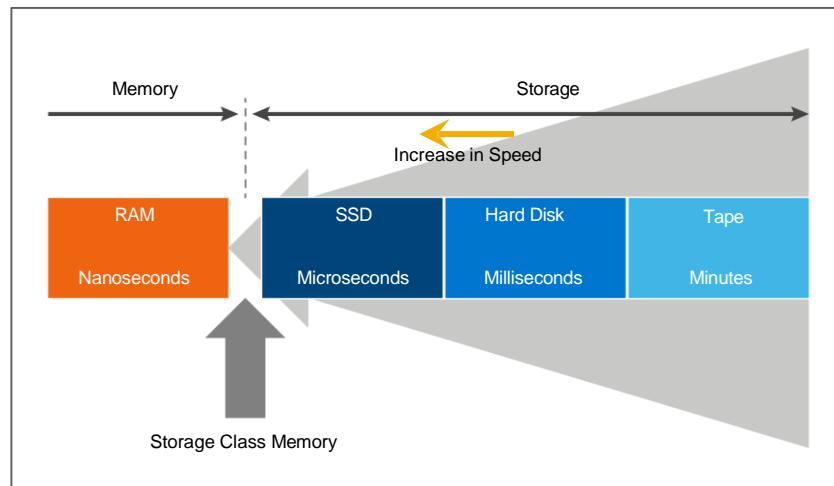
Drives with substantial amounts of their capacity consumed will take longer to complete the read-modify-write cycle. SSDs are best for workloads with short bursts of activity.

## Non-Volatile Memory Express (NVMe)



- NVMe, or non-volatile memory express, is a standardized high-performance software interface for PCI express SSDs that use nonvolatile memory (NVM).
- NVMe takes advantage of the microsecond latency that is provided by all-flash arrays and eliminates the SCSI bottleneck.
  - By reducing the latency of traditional flash-based infrastructure, NVMe can better equip organizations to manage the extreme demands of next-generation workloads.
- Offering greater storage throughput and lower latency, NVMe represents the next evolutionary step for flash storage media and next generation storage class memory media.

### Storage Class Memory



- SCM technology is a high-performance nonvolatile storage that addresses the performance needs of several latest workloads that organizations must support as part of digital transformation.
- SCM adds a new tier to the storage hierarchy, one that features memory-like performance at storage-like cost.
- SCM is slower than DRAM but read and write speeds are over 10X faster than flash and can support higher IOPS while offering comparable throughput.
- Use Case
  - Deploying SCM enables financial organizations to quickly perform data analytics on millions of records to detect fraudulent transactions.
  - It also enables organizations to quickly detect and protect against cyber threats.

#### Notes:

A data center is only as fast as its slowest link. For the past 50 years, Moore's law has continued to deliver faster and faster processors; however, the storage side has struggled to keep up. Historically, innovation in storage came gradually: first there were magnetic tapes, and then came spinning hard disk drives (HDDs) with their mechanically limited speeds. The last big leap was the adoption of NAND Flash SSDs, which cut the latency from milliseconds to microseconds. Another development was the adoption of NVMe as the default SSD interface instead of SAS.

Despite the emergence of NVMe stack, external storage systems are still orders of magnitude slower than server memory technologies (RAM). They can also be a barrier to achieving the highest end-to-end system performance.

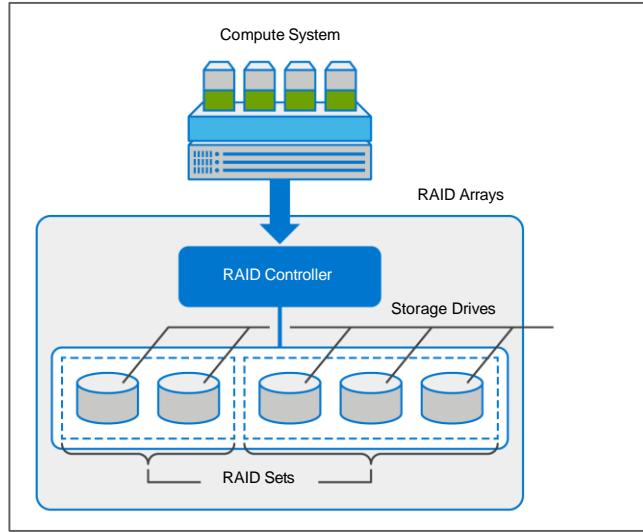
The memory industry has been aiming towards something that has the speed of DRAM but the capacity, cost, and persistence of NAND flash memory. The shift from SATA to faster interfaces such as SAS and PCI-Express using the NVMe protocol has made SSDs faster. But nowhere near the speed of DRAM.

Technologies like Phase Change Random Access Memory (PCRAM), Resistive Random-Access Memory (Re-RAM), and Magnetic Random-Access Memory (MRAM) are showing potential candidacy to be adopted as the technologies that power SCM.

RAID

## RAID

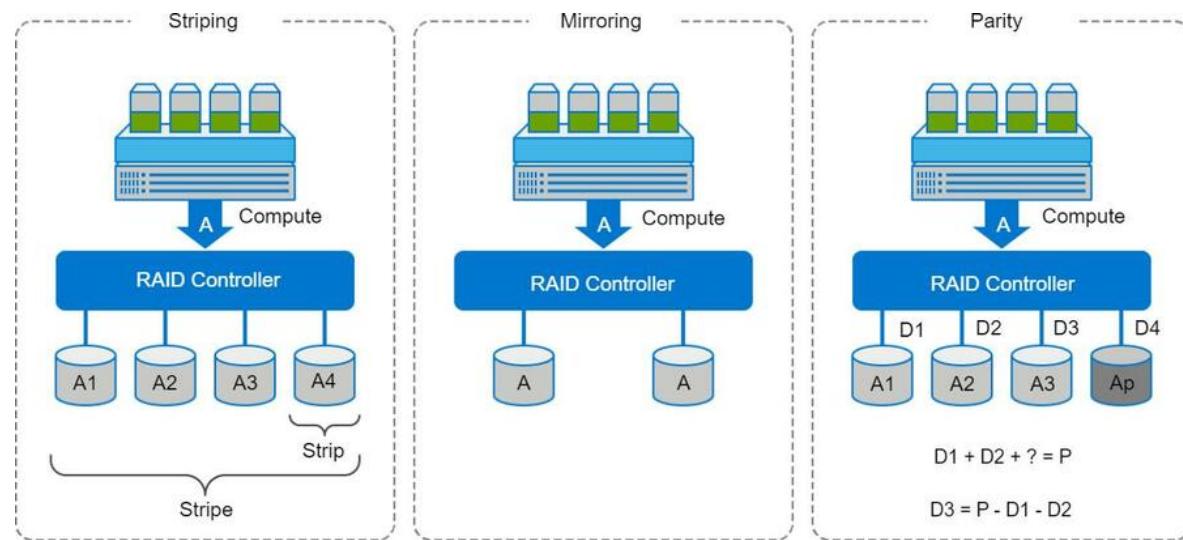
## RAID Overview



- Redundant Array of Independent Disks (RAID) is a technique that combines multiple disk drives into a logical unit (RAID set) and provides protection, performance, or both.
- RAID provides data protection against drive failures and improves storage system performance by serving I/O operations from multiple drives simultaneously.
  - RAID protects against data loss when a drive fails, by using mirroring or parity.
- A RAID array is an enclosure that contains various disk drives and supporting hardware to implement RAID.
  - A subset of disks within a RAID array can be grouped to form logical arrays, also known as a RAID set.
  - RAID is typically implemented by using a specialized hardware controller present either on the compute system or on the storage system.
  - RAID can also be implemented using software. Software RAID uses compute system-based software to provide RAID functions and is implemented at the operating-system level.

## RAID Techniques

Three different RAID techniques form the basis for defining various RAID levels.



### Notes:

**Striping** is a technique of spreading data across multiple drives in order to use the drives in parallel. All the read/write heads work simultaneously, allowing more data to be processed in a shorter time. This approach increases the performance, compared to reading and writing from a single disk. The set of aligned strips that spans across all the disks within the RAID set is called a stripe. The figure shows representations of a striped RAID set. Stripe size (also called stripe depth) describes the number of blocks in a strip (represented as "A1, A2, A3, and A4"). All strips in a stripe have the same number of blocks. Having a smaller stripe size means that the data is broken into smaller pieces while it is spread across the disks. Stripe size (represented as A) is a multiple of stripe size by the number of data disks in the RAID set. For example: in a four-disk striped RAID set with a stripe size of 64 KB, the stripe size is 256 KB (64 KB x 4). Striped RAID does not provide any data protection unless parity or mirroring is used.

**Mirroring** is a technique whereby the same data is stored on two or more disks resulting in multiple copies of the data. If one disk drive failure occurs, the data remains intact on the surviving disk drive. The controller continues to service the data requests from the surviving disk of a mirrored pair. When the failed disk is replaced with a new disk, the controller copies the data from the surviving disk of

the mirrored pair. Mirroring involves duplication of data – the amount of storage capacity that is needed is twice the amount of data being stored. Mirroring is considered expensive and is preferred for mission-critical applications that cannot afford the risk of any data loss. Mirroring improves read performance because read requests can be serviced by both disks. However, write performance is slightly lower than a single disk because each write request manifests as two writes on the disk drives.

**Parity** is a method to protect striped data from disk drive failure without the cost of mirroring. An additional disk drive is added to hold parity, a mathematical construct that allows recreation of the missing data. Parity is a redundancy technique that ensures protection of data without maintaining a full set of duplicate data. The first three disks in the figure, labeled D1 to D3, contain the data. The fourth disk, labeled P, stores the parity information, which, in this case, is the sum of the elements in each row. Now, if one of the data disks fails, the missing value can be calculated by subtracting the sum of the rest of the elements from the parity value. In the diagram, for simplicity, the computation of parity is represented as an arithmetic sum of the data. However, parity calculation is a bitwise XOR operation. For parity RAID, the stripe size calculation does not include the parity strip. For example: in a four (3 + 1) disk parity RAID set with a strip size of 64 KB, the stripe size is 192 KB (64 KB x 3).

## RAID Levels

- **RAID 0** – Striped set with no fault tolerance
  - RAID 0 configuration uses data striping techniques, where data is striped across all the disks within a RAID set.
- **RAID 1** – Disk mirroring
  - A RAID 1 set consists of two disk drives and every write is written to both disks.
- **RAID 1 + 0** – Mirroring and Striping
- **RAID 5** – Striped set with independent disk access and distributed parity
- **RAID 6** – Striped set with independent disk access and dual distributed parity

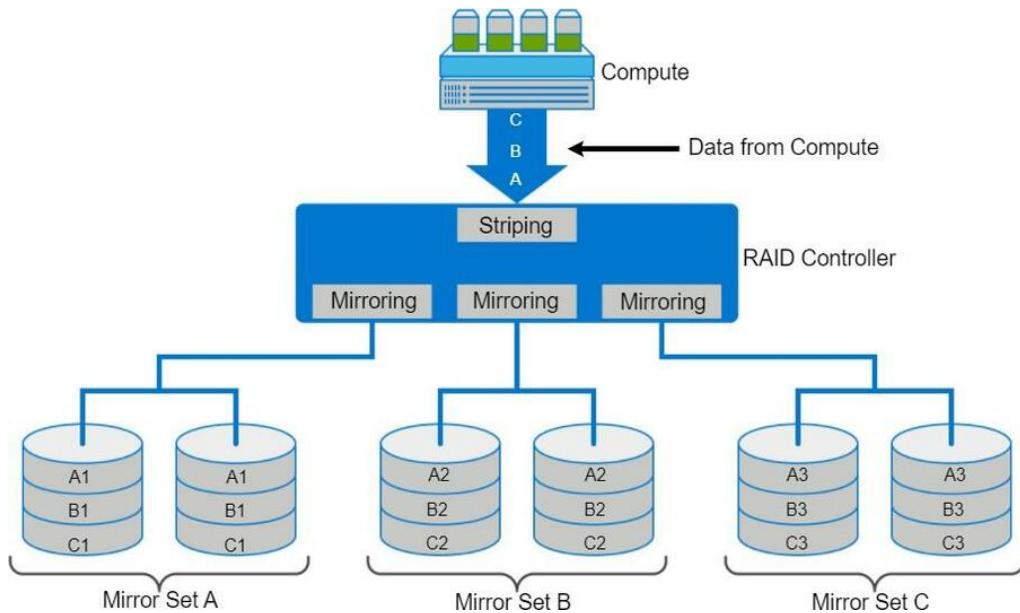
The RAID level selection depends on the parameters such as application performance, data availability requirements, and cost.

### Notes:

RAID Level	Minimum Number of Disks	Available Storage Capacity (%)	Write Penalty	Protection
1	2	50	2	Mirror
1 + 0	4	50	2	Mirror
5	3	$[(n-1)/n] * 100$	4	Parity (Supports single disk failure)
6	4	$[(n-2)/n] * 100$	6	Dual Parity (Supports two disk failures)

## RAID 1+0

RAID 1+0 uses mirroring and striping techniques and combines their benefits. This RAID type requires an even number of disks, the minimum being four.



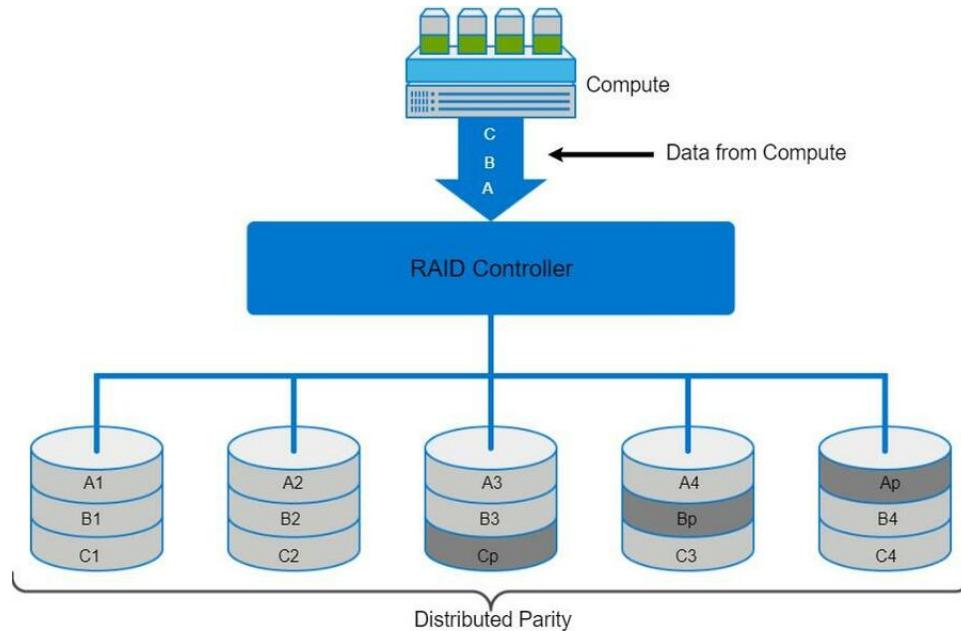
### Notes:

RAID 1+0 is also known as RAID 10 (Ten) or RAID 1/0. RAID 1+0 is also called striped mirror. The basic element of RAID 1+0 is a mirrored pair. The data is first mirrored, and then both copies of the data are striped across multiple disk drive pairs in a RAID set.

When replacing a failed drive, only the mirror is rebuilt. In other words, the storage system controller uses the surviving drive in the mirrored pair for data recovery and continuous operation. Data from the surviving disk is copied to the replacement disk.

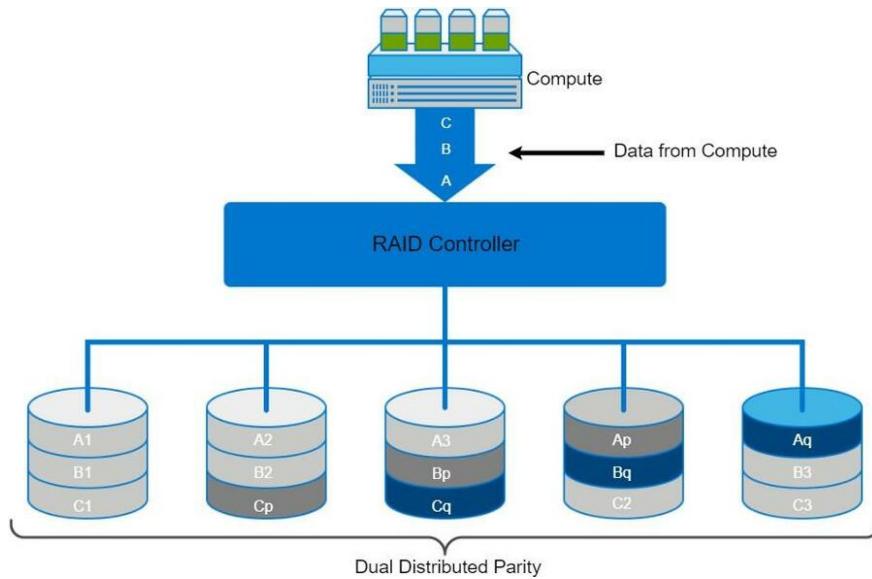
## RAID 5

- RAID 5 is a versatile RAID implementation. The drives (strips) are also independently accessible.
- In RAID 5, parity is distributed across all disks to overcome the write bottleneck of a dedicated parity disk.



## RAID 6

- RAID 6 works the same way as RAID 5. But RAID 6 includes a second parity element to enable survival when two disk failures occur in a RAID set.
  - RAID 6 implementation requires at least four disks.



### Notes:

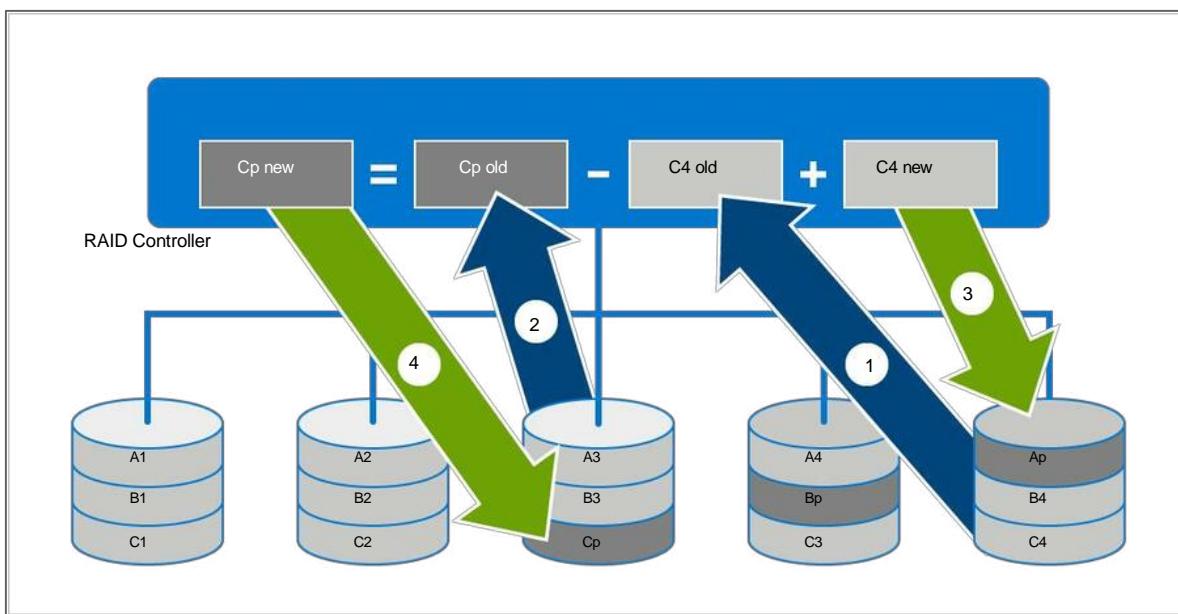
RAID 6 distributes the parity across all the disks. The write penalty (explained later in this module) in RAID 6 is more than RAID 5. RAID 5 writes perform better than RAID 6.

The rebuild operation in RAID 6 may take longer than RAID 5 due to the presence of two parity sets.

## RAID Impacts on Performance

- In RAID 5, every write (update) to a disk manifests as four I/O operations (two reads and two writes).
- In RAID 6, every write (update) to a disk manifests as six I/O operations (three reads and three writes).
- In RAID 1 and RAID 1+0, every write manifests as two I/O operations (two writes).

The figure illustrates a single write operation on RAID 5 that contains a group of five disks.



### Notes:

When choosing a RAID type, it is imperative to consider its impact on disk performance and application IOPS. In both mirrored and parity RAID configurations, every write operation translates into more I/O overhead for the disks. This process is termed as a write penalty.

In a RAID 1 implementation, every write operation must be performed on two disks that are configured as a mirrored pair. In a RAID 5 implementation, a write operation may manifest as four I/O operations. When performing I/O operations to a disk configured with RAID 5, the controller has to read, recalculate, and write a parity segment for every data write operation.

The parity (P) at the controller is calculated as follows:

$$C_p = C_1 + C_2 + C_3 + C_4 \text{ (XOR operations)}$$

Whenever the controller performs a write I/O, parity must be computed by reading the old parity ( $C_p$  old) and the old data ( $C_4$  old) from the disk. It means two read I/O operations. Then, the new parity ( $C_p$  new) is computed as follows:

$$C_p \text{ new} = C_p \text{ old} - C_4 \text{ old} + C_4 \text{ new} \text{ (XOR operations)}$$

After computing the new parity, the controller completes the write I/O by writing the new data and the new parity onto the disks. This results into two write I/O operations. The controller performs two disk reads and two disk writes for every write operation, and the write penalty is 4.

In RAID 6, which maintains dual parity, a disk write requires three read operations: two parity and one data. After calculating both the new parities, the controller performs three write operations: two parities and an I/O. In a RAID 6 implementation, the controller performs six I/O operations for each write I/O, and the write penalty is 6.

## RAID Concepts: Additional Information



*To understand more about RAID, click [here](#).*

## Knowledge Check

## Knowledge Check

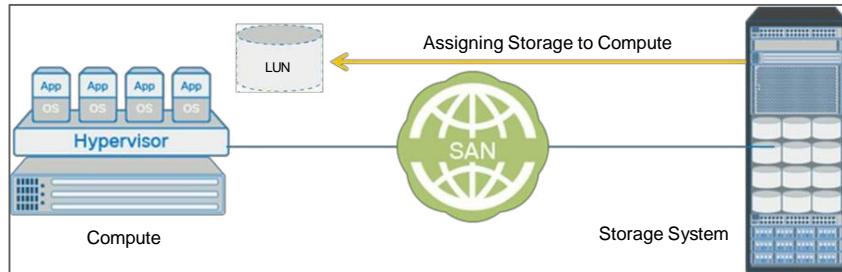
### Knowledge Check

1. Which one of the following is characteristic of RAID 5?
  - a. All parity in a single disk
  - b. No parity
  - c. Distributed parity
  - d. Double parity

# Storage Provisioning

## Storage Provisioning Overview

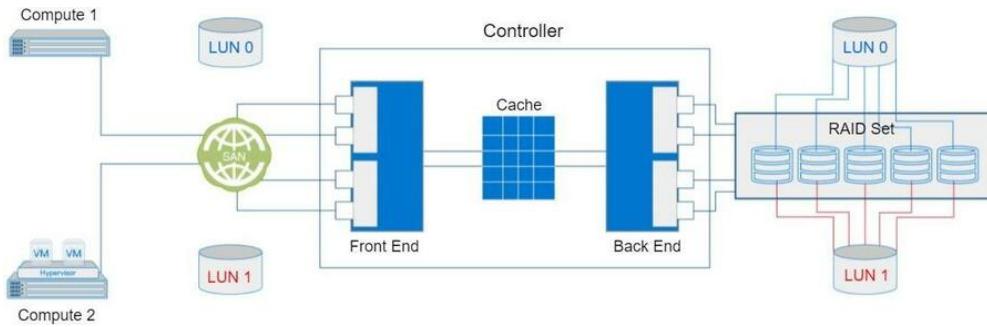
**Storage Provisioning** is the process of assigning storage resources to compute systems based on capacity, availability, and performance requirements.



- Storage provisioning can be performed in two ways:
  - Traditional
  - Virtual
- Virtual provisioning leverages virtualization technology for provisioning storage.

## Traditional Provisioning

The image shows a RAID set consisting of five storage drives that have been sliced or partitioned into two LUNs<sup>38</sup>: LUN 0 and LUN 1. These LUNs are then assigned to Compute 1 and Compute 2 for their storage requirements.



- For traditional provisioning, the number of drives in the RAID set and the RAID level determine the availability, capacity, and performance of the RAID set.
  - It is highly recommended to create the RAID set from drives of the same type, speed, and capacity. This approach ensures maximum usable capacity, reliability, and consistency in performance.

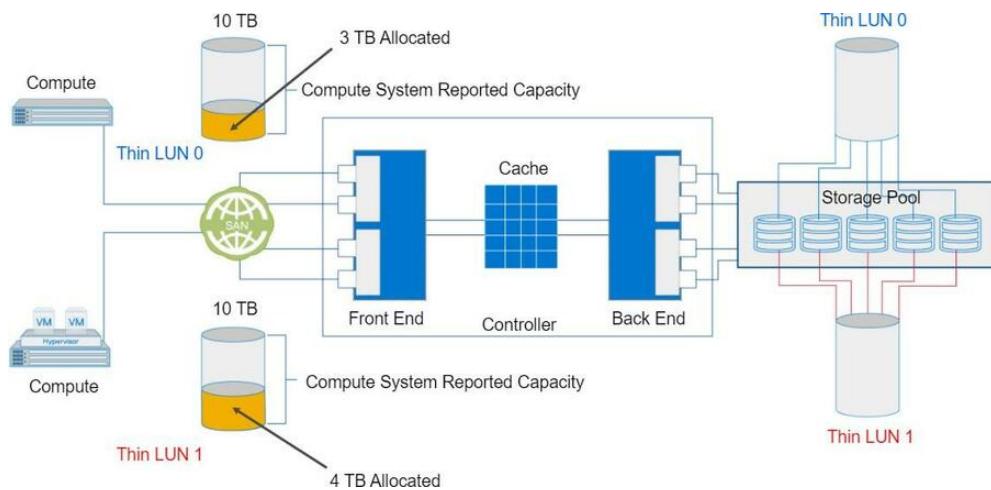
---

<sup>38</sup> Each logical unit that is created from the RAID set is assigned a unique ID, called a logical unit number (LUN). LUNs hide the organization and composition of the RAID set from the compute systems. LUNs created by traditional storage provisioning methods are also termed as thick LUNs to distinguish them from the LUNs created by virtual provisioning methods.

### Virtual Provisioning

Virtual provisioning enables creating and presenting a LUN with more capacity than is physically allocated to it on the storage system.

The LUN created using virtual provisioning is called a thin LUN<sup>39</sup> to distinguish it from the traditional LUN (Thick LUN<sup>40</sup>).



#### Notes:

Physical storage is allocated to the compute system “on-demand” from a shared pool of physical capacity. A shared pool consists of physical storage drives.

---

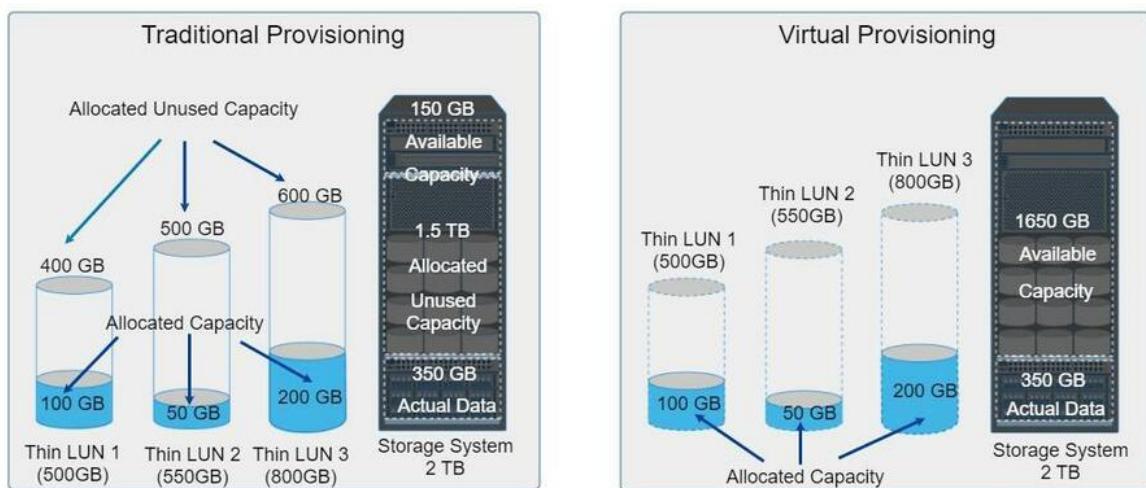
<sup>39</sup> Thin LUNs do not require all the physical storage to be allocated to them at the time they are created and presented to a compute system. Thin LUN only uses the physical storage as needed in increments.

<sup>40</sup> Thick LUNs require all the physical storage that is allocated to them at the time they are created and presented to a compute system.

Virtual provisioning enables more efficient allocation of storage to compute systems. Virtual provisioning also enables oversubscription, where more capacity is presented to the compute systems than is physically available on the storage system. Both the shared pool and the thin LUN can be expanded nondisruptively as the storage requirements of the compute systems grow. Multiple shared pools can be created within a storage system, and a shared pool may be shared by multiple thin LUNs.

### Traditional Provisioning vs. Virtual Provisioning

- Traditional Provisioning
  - Administrators typically allocate storage capacity that is based on anticipated storage requirements. This generally results in the over provisioning of storage capacity, which then leads to higher costs and lower capacity utilization.
- Virtual Provisioning
  - It improves storage capacity utilization and simplifies storage management.



#### Notes:

With traditional provisioning, three LUNs are created and presented to one or more compute systems. The total storage capacity of the storage system is 2 TB. The allocated capacity of LUN 1 is 500 GB, of which only 100 GB is consumed, and the remaining 400 GB is unused. The size of LUN 2 is 550 GB, of which 50 GB is consumed, and 500 GB is unused. The size of LUN 3 is 800 GB, of which 200 GB is consumed, and 600 GB is unused.

In total, the storage system has 350 GB of data, 1.5 TB of allocated but unused capacity. It has only 150 GB of remaining capacity available for other applications. Now consider the same 2 TB storage system with virtual provisioning. Here, three thin LUNs of the same sizes are created. However, there is no allocated unused capacity. In total, the storage system with virtual provisioning has the same 350 GB of data. But 1.65 TB of capacity is available for other applications, whereas only

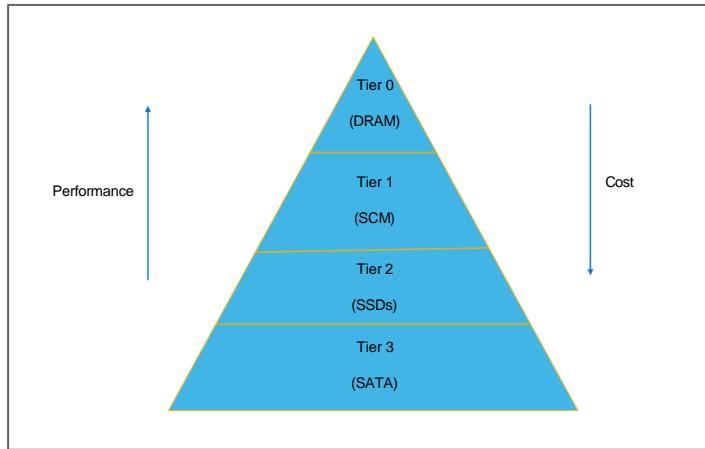
150 GB is available in traditional storage provisioning. This approach improves the overall utilization of storage resources and reduces the storage cost.

Thin LUNs are appropriate for applications that can tolerate performance variations. Sometimes, performance improvement is perceived when using a thin LUN, due to striping across many drives in the pool. However, when multiple thin LUNs contend for shared storage resources in a given pool, and when utilization reaches higher levels, the performance can degrade. Thin LUNs provide the best storage space efficiency and are suitable for applications where space consumption is difficult to forecast. Traditional LUNs are suited for applications that require predictable performance.

Storage Tiering

## Storage Tiering

## Storage Tiering Overview



Storage tiering is a technique of establishing a hierarchy of storage types. Also, identifying the candidate data to relocate to the appropriate storage type to meet service level requirements at a minimal cost.

- Each tier has different levels of performance and cost.
- Efficient storage tiering requires defining tiering policies.

### Notes:

Storage tiering can happen within and across storage systems. Each tier has different levels of protection, performance, and cost. For example, high-performance SSDs or SCM can be configured as tier 1 storage to keep frequently accessed data. FC drives<sup>41</sup> as tier 2 storage, and low-cost SATA drives as tier 3 storage to keep the less frequently accessed data.

---

<sup>41</sup> Disk drives are accessed through predefined protocols, ATA, SATA, SAS, and FC. These protocols are implemented on the disk interface controllers. Typically, disk interface controllers are integrated with the disk drives. So the disk drives are

## Storage Tiering

Keeping frequently used data in SSD or SCM improves application performance. Moving less-frequently accessed data to low-cost SATA can free up storage capacity in high-performance drives and reduce the cost of storage. This movement of data happens based on defined tiering policies. The tiering policy might be based on parameters, such as frequency of access.

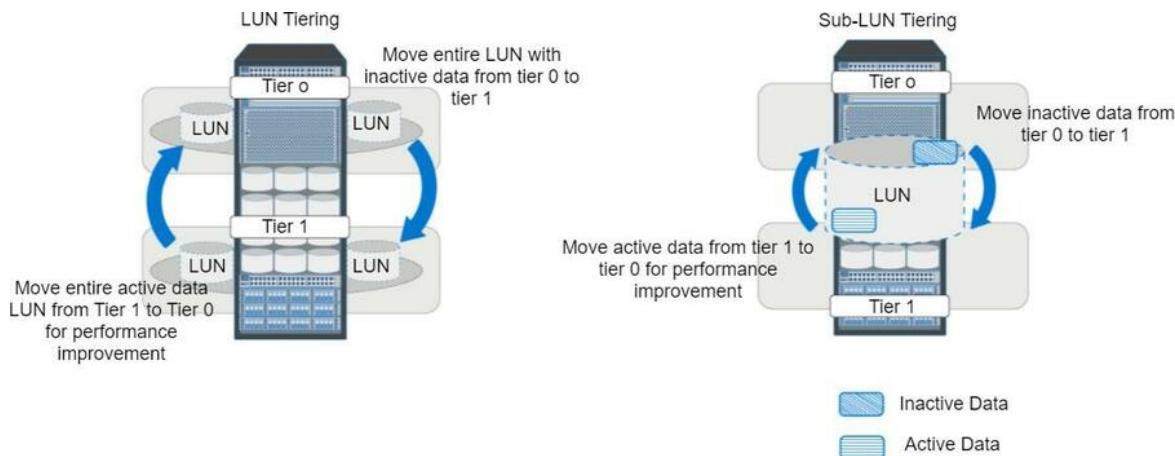
For example, a policy states "move the data that are not accessed for the last 120 minutes to the lower tier." All the data matching this condition are moved to the lower tier within a storage system. Take another case: a policy states "move the data that are not accessed for the last 60 days to the cloud." All the data matching this condition are moved to the cloud.

---

known by the protocol interface they support. For example, SATA disk, and FC disk.

## Tiering Within a Storage System

- The process of storage tiering within a storage system is called intra array storage tiering.
  - It enables the efficient use of SSD, FC, and SATA drives within a system and provides performance and cost optimization.
- Data movements that are performed between tiers can be performed at the LUN level<sup>42</sup> or at the sub-LUN<sup>43</sup> level.



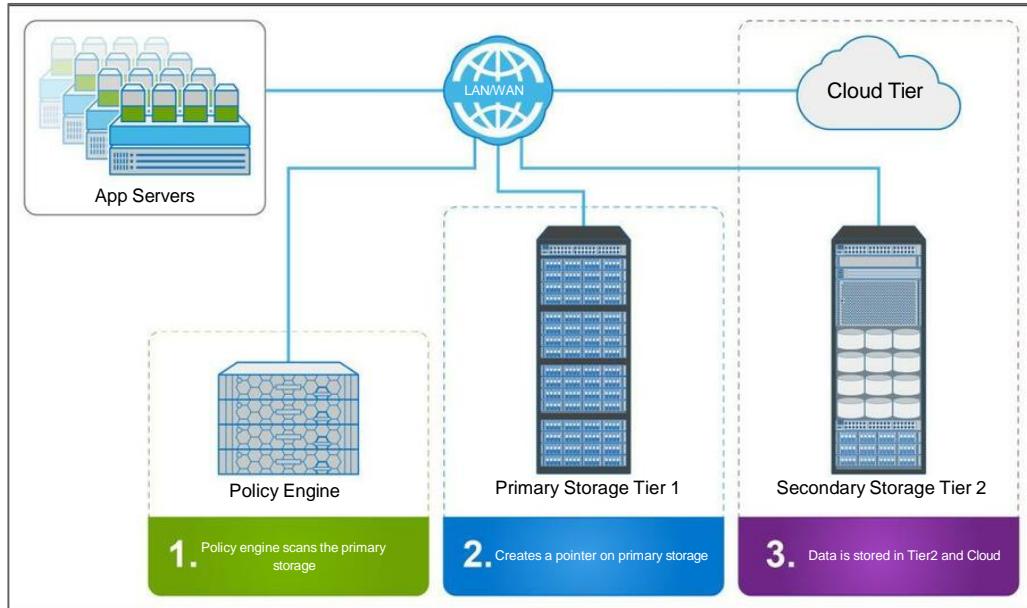
<sup>42</sup> Moves entire LUN from one tier to another. Does not give effective cost and performance benefits.

<sup>43</sup> A LUN is broken down into smaller segments and tiered at that level. Provides effective cost and performance benefits.

## Storage Tiering

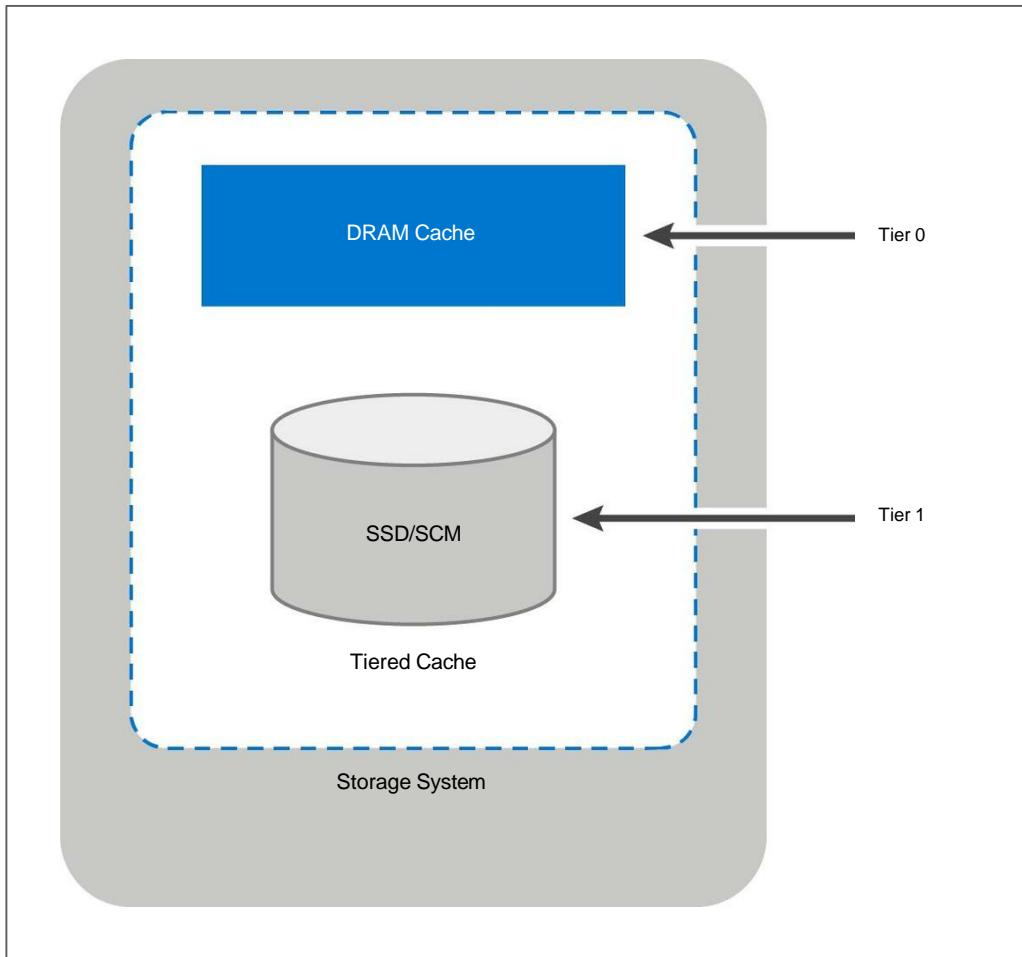
### Tiering Between Storage Systems

- In this storage tiering environment, data can be moved to a secondary storage tier or to the cloud.



- Before moving data from primary storage to secondary storage or from primary storage to cloud, the policy engine scans the primary storage to identify data that meet the predefined policies.
- After identifying the data, the pointers are created, and the data is moved to the destination storage tier.

## Cache Tiering



- Cache tiering enables creation of a large capacity secondary cache using SSD and SCM.
- It enables tiering between DRAM cache and SSD/SCM (secondary cache).
- Most reads are served directly from high-performance tiered cache.
- Cache tiering enhances performance during peak workloads.

## Storage Tiering: Additional Information



*To understand the storage tiering concepts, click [here](#).*

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. What is a benefit of implementing storage tiering?
  - a. Improves deduplication performance
  - b. Reduces storage cost
  - c. Eliminates the need of hard disk drives
  - d. Improves the performance of hard disk drives

# Block, File and Object-based Storage Systems

## Knowledge Check

### Block, File and Object-Based Storage Systems

## Block-Based Storage Systems

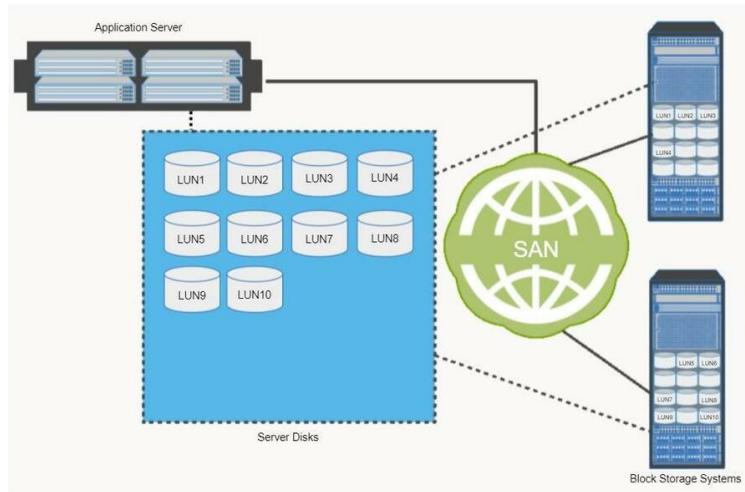
## Block, File, and Object-Based Storage Systems

The main objectives of the module are to:

- Describe the architecture, components, operations, and use of each storage system type.
- Explain the advantages of unified storage systems to store and serve block and file-based data.

## Block-Based Storage Systems

### Block-Based Storage System Overview



*Block-based storage systems LUNs appear to the server as internal physical disks. (Click to enlarge.)*

Data is stored on disk devices in blocks containing a fixed number of bytes.

Typically, a data block contains 512 or 4,086 bytes.

- Block disk devices store raw data only. Metadata, such as a file system, is maintained in the operating system.
- The file system is a directory to the block data on storage systems.
- Block-based storage systems can have either a scale-up or scale-out architecture.
- Block-based storage systems offer data protection, replication, and other capabilities.

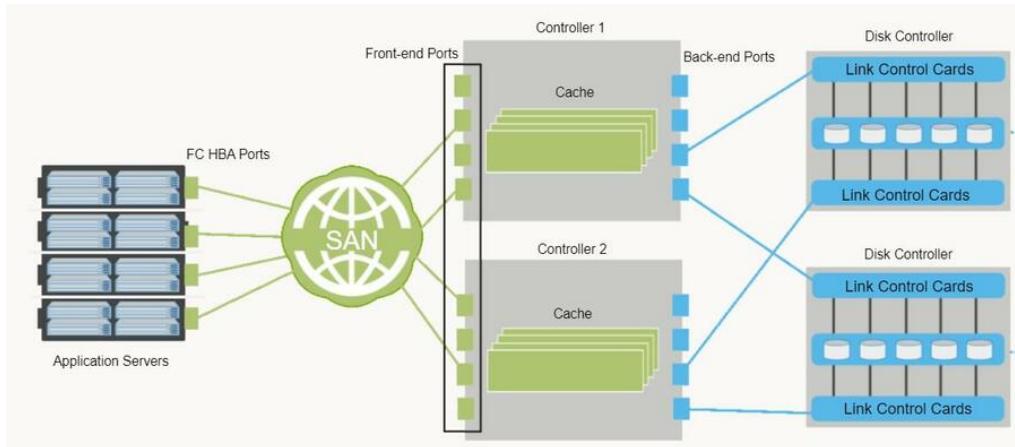
## Block Storage System Components

All block-storage systems are designed using the four main storage system components regardless of manufacturer or model. All storage components are contained within, or connected to the [storage controllers](#).

### Front-end Ports

The front-end ports connect hosts to the storage system. Hosts connect only through the front-end ports. They do not have direct access to any other devices of the storage system. Front-end ports are attached to front-end controllers. Front-end ports provide the connectivity protocol logic such as Fibre Channel or iSCSI, or for mainframes hosts, the ESCON or FICON protocols. Depending on host interface connectivity configuration, front-end port block I/O is processed through either or both storage controllers.

The image shows four hosts, each with one FC HBA port. Dual redundant connections to both storage controllers are still achieved, as it is configured through a Fibre Channel Storage Area Network (SAN). For complete, end-to-end connection redundancy, each host should be equipped with at least two FC HBA ports.



### Cache

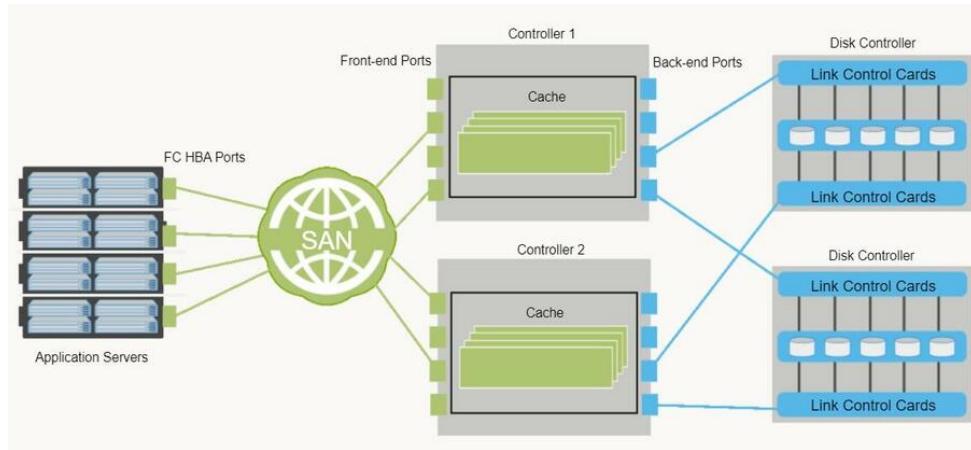
Storage system controllers contain high speed DRAM memory. Used as an active cache, the DRAM buffers inbound data before writing to disk, and buffers outbound

## Block-Based Storage Systems

data from disks to hosts. Placing DRAM memory between storage system disks and front-end ports increases I/O performance.

Both storage controllers contain the same amount of embedded cache in the form of DRAM memory modules. The cache in the path between the disk array back-end ports and the host front-end ports. In this location, all read and write block I/O must pass through the cache, increasing read and write I/O performance.

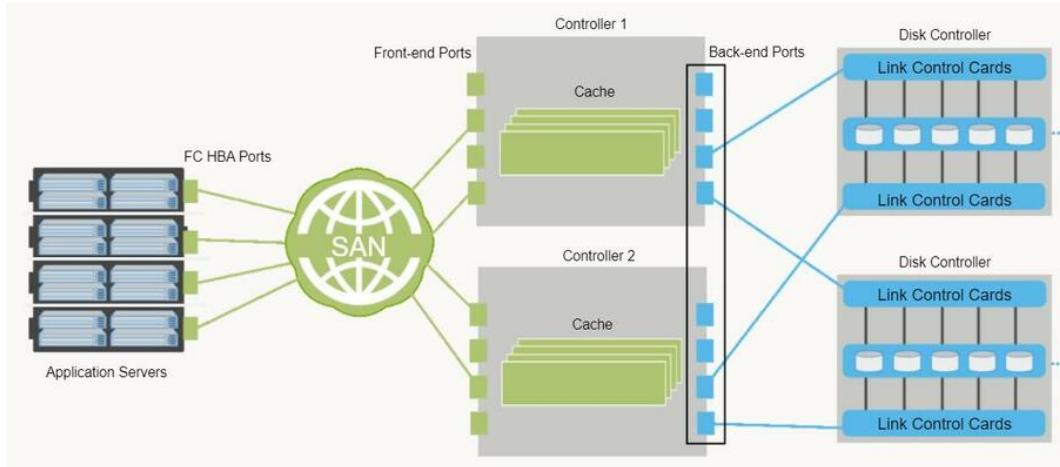
I/O performance acceleration can be increased and scale further to benefit the addition of hosts and storage by adding more cache memory to the controllers.



### Back-end Ports

Back-end ports connect through the link control cards to the shelves of physical disk and devices in each disk array enclosure (DAE). Dual redundant connections between the controllers and all DAEs provide disk I/O reliability. Unused back-end ports are available to connect additional DAEs to the system.

## Block-Based Storage Systems

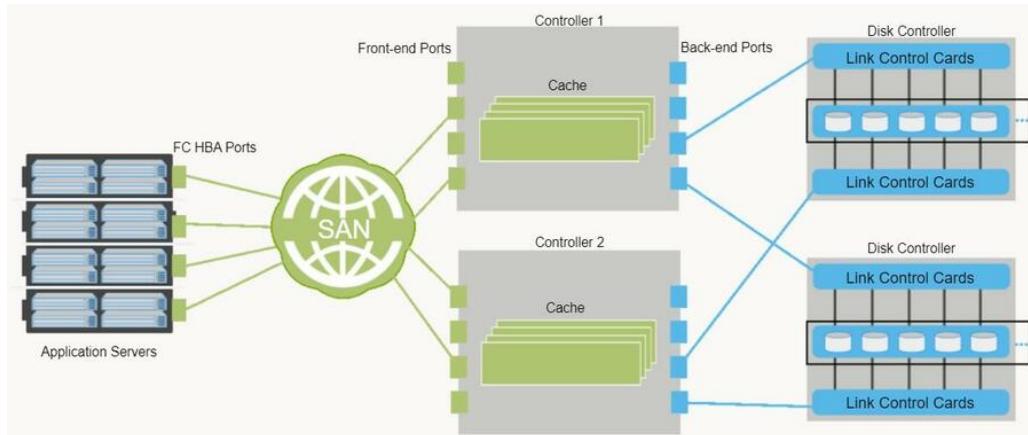


### Disk Array

The disk array contains traditional hard disk drives or solid state drives. These devices are only accessible by the storage system controllers.

The disk array provides physical block storage capacity to the storage system. The devices are arranged in shelves within a DAE.

Scaling, higher storage capacity, and I/O performance are achieved by adding DAEs.



### Notes:

A **storage controller** is the device within the storage system that operates and manages all of the functional components of the system. Storage systems should have a minimum of two storage controllers. This arrangement provides operational redundancy, and enhances I/O performance and scalability. Storage Controllers:

## Block-Based Storage Systems

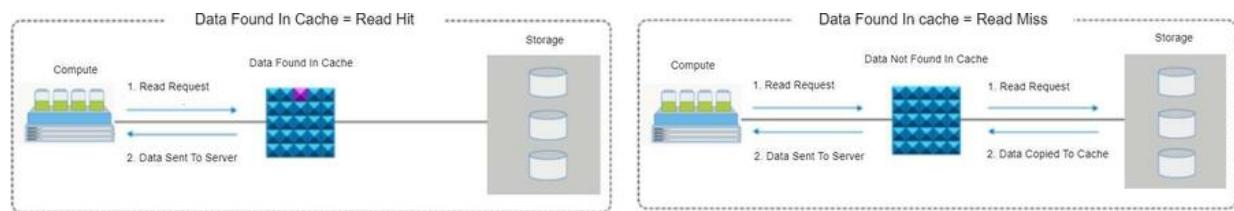
- Contain **front-end ports** to connect to a SAN or directly to servers.
- Contain back-end ports that connect to the internal disk array enclosures.
- Implement hardware RAID to logically segment disk drives. Presents the segments to servers as logical block disk devices or LUNs.
- Contain and manage the DRAM **cache** memory that accelerates host and internal disk array read and write I/O.

Storage controllers are sometimes referred as RAID controllers, or by different names assigned by the system manufacturer. For example, Dell EMC Unity controllers are named Storage Processor A and Storage Processor B (SPA, SPB). PowerMax controllers are named Director 1 and Director 2.

## Cache Operations

**How cache is used to increase host read I/O performance:**

- Host sends read request to the front-end port. If requested data is in cache, then the data is quickly sent from its cache location to the front-end port back to the host. Fetching requested data that is already in cache is known as a Read hit<sup>44</sup>.
- Host sends read request to the front-end port. If requested data is not in cache, the request is forwarded through the back-end ports, and the link controller to the disk devices. Data is fetched from the disks and takes the same route back to the host. Fetching requested data that is not already in cache is known as a Read miss<sup>45</sup>.



*The image compares cache read hit and read miss operations*

**Cache Write I/O Operations:**

<sup>44</sup> The storage controller stores the requested data in cache to increase the chances of a read hit when next requested.

<sup>45</sup> A Read Miss requires read data to traverse the longer end-to-end I/O path to disk. It must be read and processed at each storage system component which adds latency. Also, disk device access times are very slow compared to cache memory.

## Block-Based Storage Systems

- **Write-Back Operation:** Write data in the cache of both controllers eventually must be written to the disk devices. Writing to disk can be done later because there is no impact to host I/O performance. Typically, the storage system schedules write to disk during low host activity or idle time.
- **Write-Through Operation:** Write data passes through the cache, and immediately written to the disk devices. An acknowledgment is sent to the host after the data is written to disk. Because data is committed to disk as it arrives, the risks of data loss is low, but write-response time is longer due to bypassing the speed of storing data in cache before de-staging to disk.

## Block Storage System Disk Drive Protocols

Intelligent storage systems provide support for a variety of disk devices of different speeds and types, such as FC, SATA, SAS, and solid state (SSD) disk devices. They also support the using a mix of SSD, FC, or SATA within the same storage system. Additionally, enterprise storage systems support disk devices that use the NVM Express (NVMe) protocol.

### FC

Fibre Channel is a high-speed block data transfer protocol. Along with high performance, FC guarantees in-order delivery of data block data read from the disk device. FC disk drives are design to provide high performance over storage capacity.

### SAS

Serial Attached SCSI is a block disk protocol that replaced parallel SCSI disk drive connectivity. SAS disk drives are designed for midrange block I/O storage applications, balancing performance with higher storage capacity requirements.

### SATA

Serial Advanced Technology Attachment is a block disk protocol that is typically used in less demanding block storage I/O applications. SATA disk drives are less expensive and provide higher storage capacity than FC or SAS disk drives.

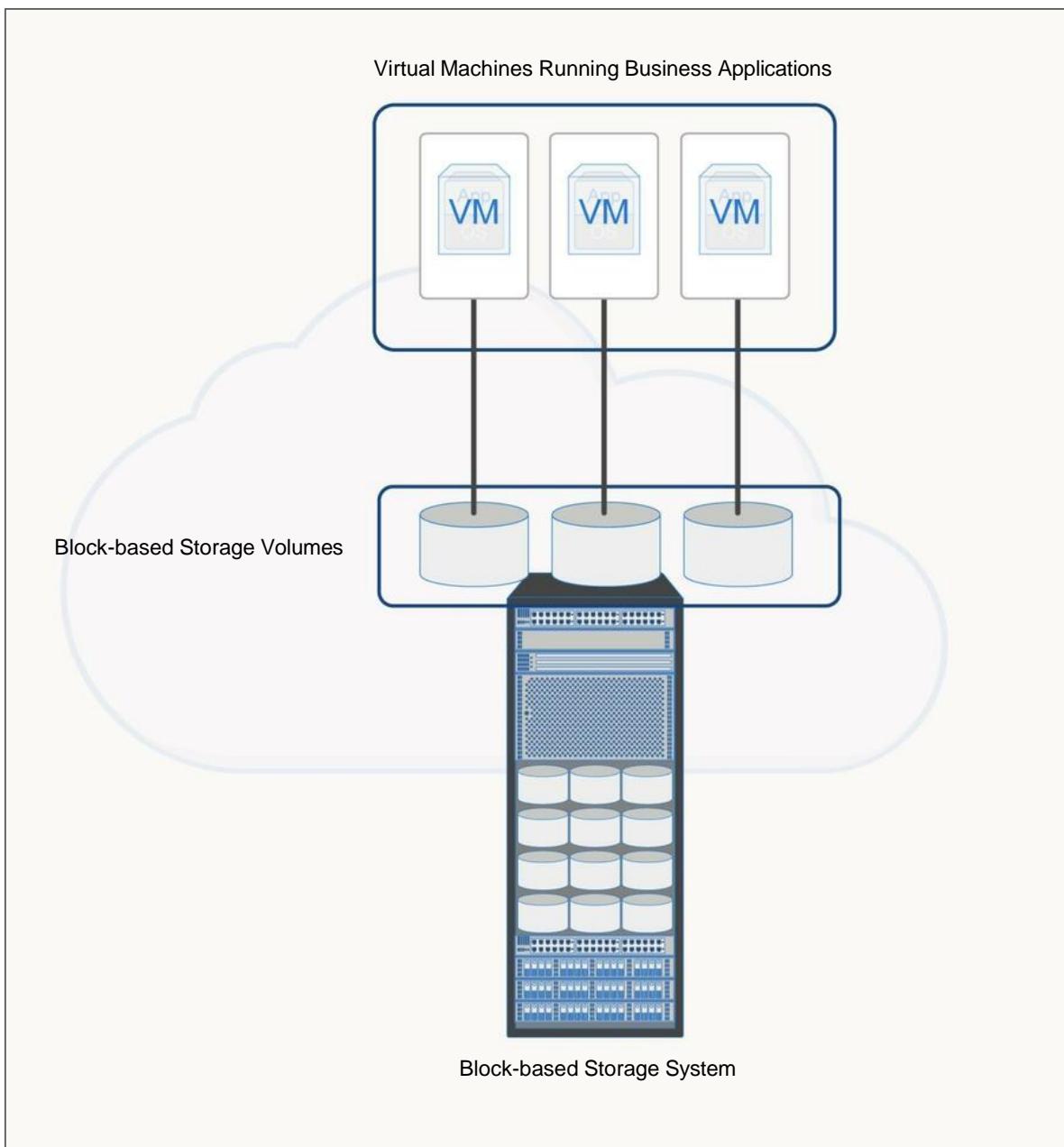
### NVMe

Nonvolatile Memory Express is an optimized block disk connectivity protocol provides the highest block I/O transfer rates and lowest latency of all block-based storage protocols. It is designed to allow enterprise class SSD storage devices to operate at their maximum performance.

## SSD

Solid-state disk devices are the highest performing and most expensive of all disk devices. SSD devices can use SATA or NVMe interface protocols for connectivity. SSD devices are used where highest I/O performance is more important than storage capacity. Using the SATA protocol interface with SSD devices suppresses their high I/O performance capability.

## Use Case - Block-Based Storage in the Cloud



### Storage as a Service

To develop prototypes or to quickly scale to meet user demand, organizations may move their application to a public cloud. To ensure proper functioning of the application and provide acceptable performance, service providers offer block-based storage in cloud.

## Block-Based Storage Systems

The service providers enable the consumers to create block-based storage volumes and attach them to the virtual machine instances. After the volumes are attached, consumers can create the file system on these volumes and run applications the way they would on an on-premises data center.

## Knowledge Check

## Knowledge Check

### Knowledge Check

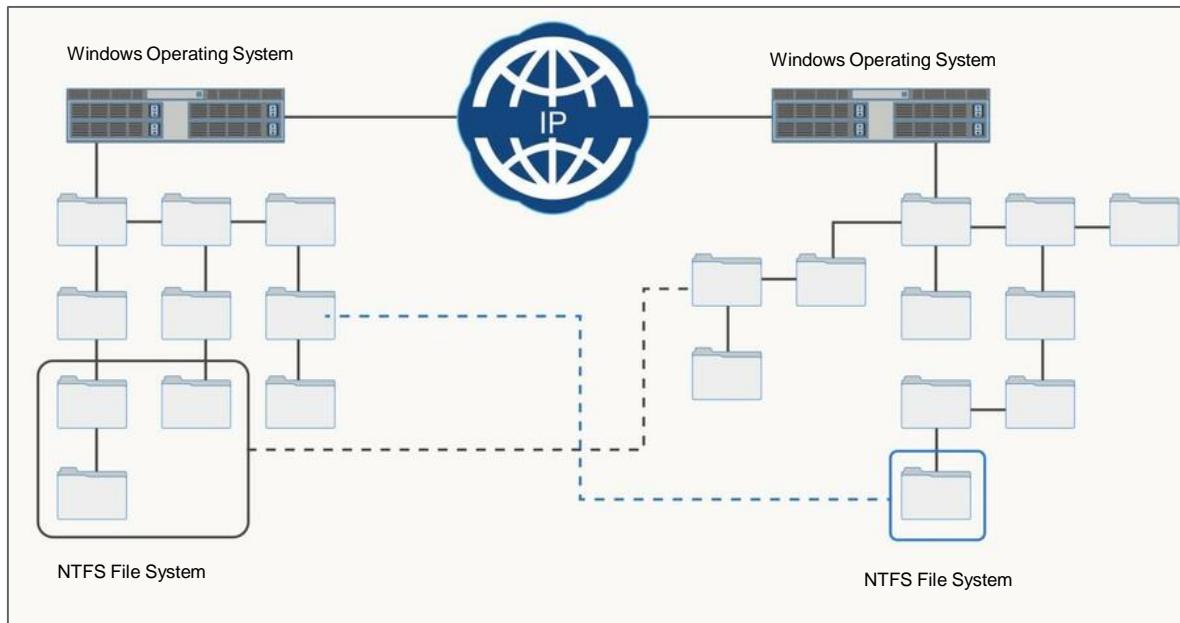
1. What is a characteristic of block data storage?
  - a. Data bytes written to disk devices are stored in blocks of a consistent size.
  - b. Data bytes written to disk devices are stored in blocks of variable size.
  - c. Data blocks written to disk devices are stored in bytes of variable size.
  - d. Data blocks written to disk devices are stored in bytes of a consistent size.

## Knowledge Check

## File-Based Storage Systems

## File-Based Storage System (NAS)

### File Systems and Network File Sharing



*With file sharing enabled, folders virtually become a part of the hierarchy of another file system.  
Shared folders appear as locally stored.*

Applications access data in the form of *files*. A file has metadata so an application or user can correctly access, and use the raw, block file data. Metadata<sup>46</sup> add other important information that is associated with the file datatype.

---

<sup>46</sup> In computer files, metadata is additional data that describes the raw data in the file. For example when a digital photo editor opens a file, it first reads the metadata to ensure the raw data is a digital photo in the correct format, such as JPG or PNG. The photo editor also reads the metadata to understand details about the image, such as its height and width, pixel density, and the type of compression used to store the raw data on disk.

- File names, extensions, and metadata are organized, and maintained by the host operating system in the form of a file system<sup>47</sup>.
- Each server has its own file system. The file system is only accessible to that server.
  - File sharing functionality is integrated, but must be enabled. Enabling file sharing allows access by other hosts. The creator or owner of each file determines the type of access to be given to other users.

### Notes:

The benefits of network file sharing degrades as more general purpose servers are added to share file system data with each other, and client systems. The major problems with network file serving are:

- **Lack of Scalability:** File server processing demands and complexity increase rapidly as more servers and growing file systems are added to the sharing pool. Performance decreases as the sharing environment increases.
  - **File System Incompatibilities Across Operating Systems:** Windows file systems are based on different protocols than Linux file systems. Cross operating system file sharing requires complex folder and file metadata
- 

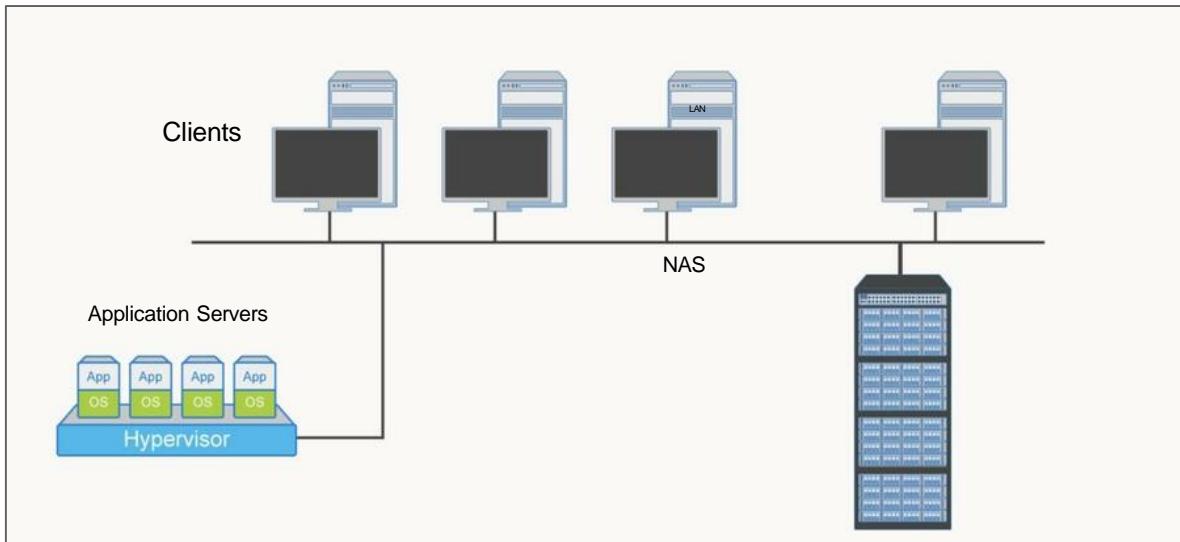
<sup>47</sup> A file system is a logical representation of how an operating system manages where and how data is stored on disk drives. Files are typically stored in folders, and folders are organized in a hierarchical tree-like structure that can be directly accessed or searched sequentially for files. A file system also contains metadata about file and folder size, names, file data location on disk drives, date and time accessed, modified, etc. File metadata also describes how an application or user can access the raw data in the correct format. There are different file system types that add additional features and functions, such as deduplication, compression, distributed access across clustered hosts, and rapid search capabilities.

## File-Based Storage Systems

mapping and conversions where Windows and Linux applications and users must access files across their native file systems.

- **Complex File Sharing Administration and Data Maintenance:** Each file server, and their file system, folders and files must be administered individually. Individual server and file system administration and maintenance requirements is prone to causing errors that can compromise data integrity, access and security problems.

## File-Based Storage Systems: Network Attached Storage (NAS)



File-based storage systems are purpose-built, high performance, high scalability platforms that take the place of general-purpose servers to store and share file data. These specialized storage systems are known as **Network Attached Storage (NAS)** systems.

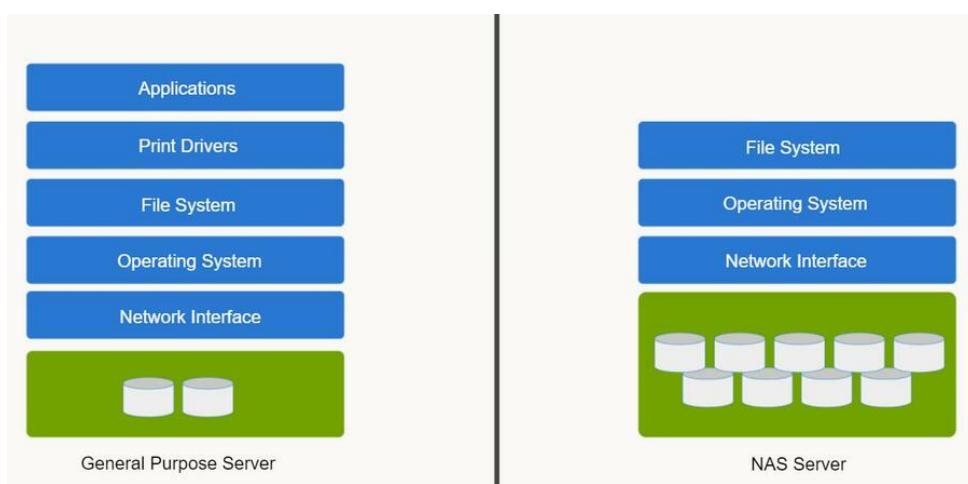
NAS provides the advantages of server consolidation by storing all file data from the general-purpose servers into its own file systems. File server consolidation makes it easier to manage the storage.

- Centralizes and optimizes file sharing operations, administration, and management.
- Uses specialized operating system that is optimized for file I/O.
- Enables Linux, UNIX, and Windows users to share data more efficiently.

### General Purpose Servers Vs. NAS Systems

A NAS system is optimized for file-serving functions such as storing, retrieving, and accessing files for applications and clients; as shown on the image:

- A general-purpose server can be used to host any application because it runs a general-purpose operating system.
- Unlike a general-purpose server, a NAS device is dedicated to file-serving.
- It has a specialized operating system that is dedicated for file serving by using industry standard protocols. NAS vendors also support features, such as clustering<sup>48</sup> for high availability, scalability, and performance.



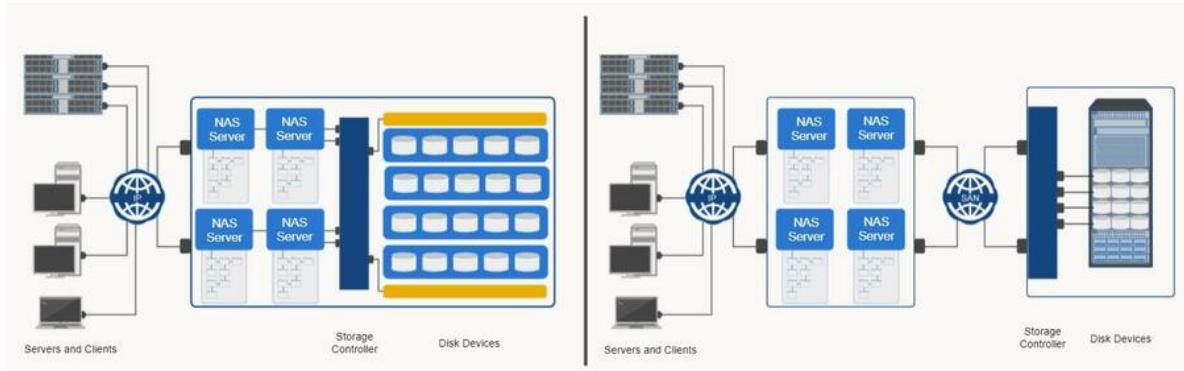
*NAS servers do not run user applications nor access user peripheral devices*

<sup>48</sup> The clustering feature enables multiple NAS controllers, heads, or nodes to function as a single entity. The workload can be distributed across all the available nodes. Clustering enables NAS to support massive workloads.

## NAS Components

NAS systems consist of NAS controllers and storage. For smaller applications, NAS controllers can reside in the same physical unit as the storage controllers and disk array.

- A NAS controller consists of:
  - CPU, memory, network adapters, and so on.
  - Specialized operating systems installed.
- Storage
  - Supports different types of storage devices.
  - Storage can be integrated with the NAS system or be connected through a SAN.



*The image on the left shows an integrated NAS system. The image on the right shows multiple NAS Servers with external SAN storage*

### Notes:

A NAS system consists of two components, controller and storage.

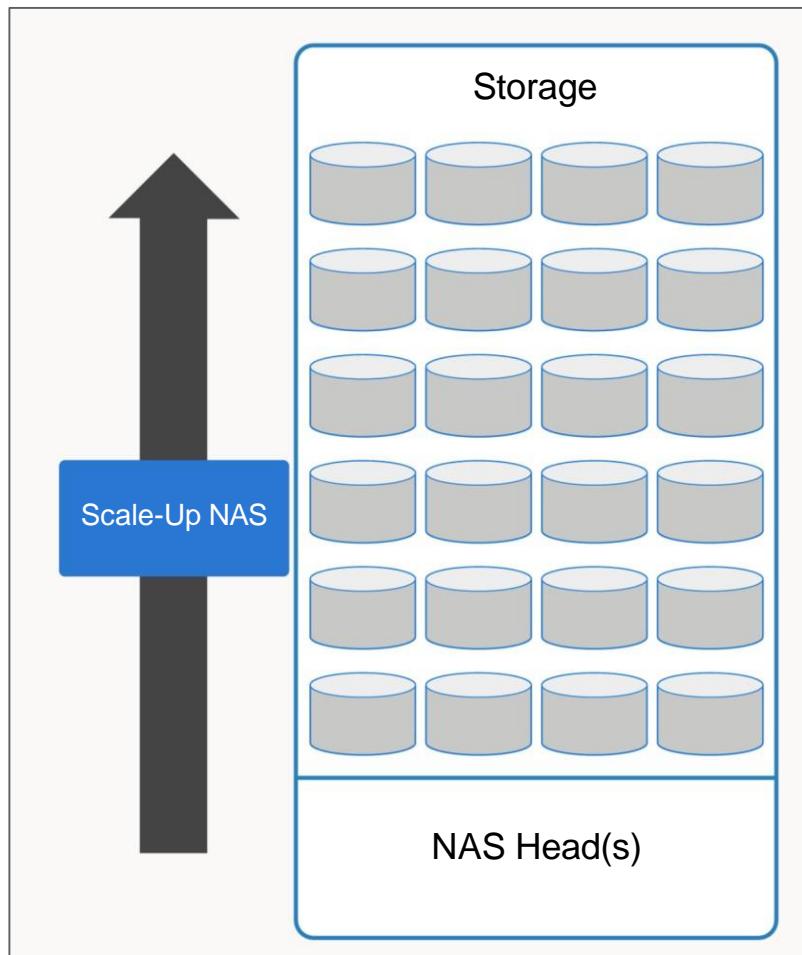
- **NAS Controllers:** A NAS controller is a compute system that contains components such as network, memory, and CPU resources. A specialized operating system optimized for file serving is installed on the controller. Each controller may connect to all storage in the system. The controllers can be active/active, with all controllers accessing the storage, or active/passive with some controllers performing all the I/O processing while others act as spares. A spare is used for I/O processing if an active controller fails. The controller is

## File-Based Storage Systems

responsible for configuration of RAID set, creating LUNs, installing file system, and exporting the file share on the network.

- **File Data Storage:** Similar to general purpose servers, block-based storage is used to store NAS raw file data, and metadata. Block storage controllers and devices are integrated into the NAS system enclosure. To provide scalability and higher capacities, midrange to enterprise NAS systems connect to external high performance block-based storage systems over iSCSI or FC SAN.
- **Disk Devices:** Integrated NAS, and NAS heads can use different types of disk devices to support mixed I/O performance and capacity requirements. NAS systems of each type can support SSD, SAS, and SATA disk devices simultaneously to add data tiering capability.

## Scale-Up NAS



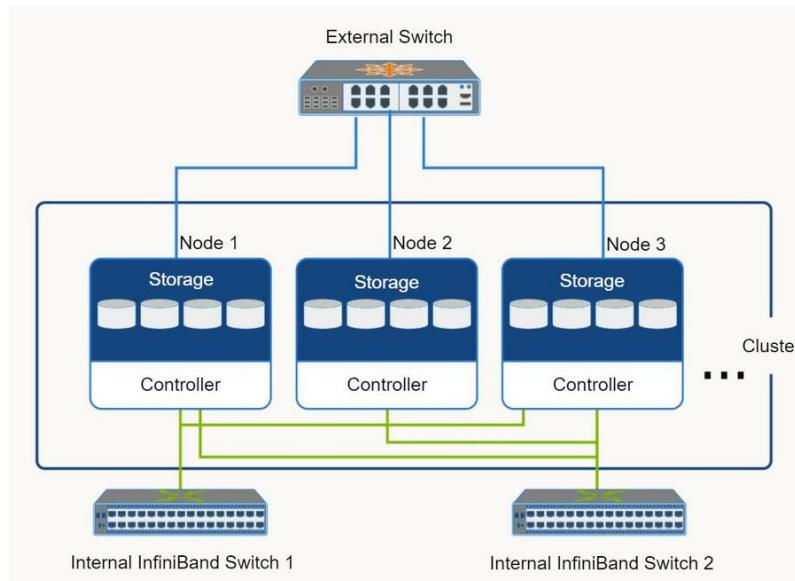
Scale-Up architecture provides the ability to independently grow capacity and performance. For example, if you only added storage to a system you'd be scaling up. Or if you only added NAS Controllers that contained CPU and memory, you'd be scaling up.

NAS systems have a fixed capacity ceiling, which limits their scalability. The performance of these systems starts degrading when reaching the capacity limit.

### Scale-Out NAS

Scale-Out is the ability to grow capacity and performance simultaneously. For example, adding a node to a NAS system adds additional CPU, Memory, Network Adapters and Storage. Adding a node would be an example of Scale-Out.

Scale-out NAS:



- Pools multiple NAS servers or *nodes* in a cluster to work as a single NAS device.
- Scales performance and capacity non-disruptively.
- Creates a single file system that runs on all nodes in the cluster.
  - Clients, which are connected to any node can access the entire file system.
  - File system grows dynamically as nodes are added.
- Stripes data across nodes with mirror or parity protection.

#### Notes:

The scale-out NAS implementation pools multiple NAS nodes together in a cluster. A node may consist of either the NAS head or the storage or both.

- A node may consist of either the NAS head or the storage or both. The cluster performs the NAS operation as a single entity.

- Scale-out NAS has the capability to scale resources by adding nodes to a cluster.
  - Nodes can be added to the cluster for more performance or storage capacity without causing any downtime.
- The cluster works as a single NAS device and is managed centrally.
- All information is shared among nodes, so the entire file system is accessible by clients connecting to any node in the cluster.
  - Scale-out NAS stripes data across all nodes in a cluster along with mirror or parity protection. As nodes are added, the file system grows dynamically. Data is evenly distributed across the nodes.
- As data is sent from clients to the cluster, the data is divided and allocated to different nodes in parallel.

Scale-out NAS clusters use separate internal and external networks for back-end and front-end connectivity respectively. An internal network provides connections for intra-cluster communication, and an external network connection enables clients to access and share file data.

Each node in the cluster connects to the internal network. The internal network offers high throughput and low latency and uses high-speed networking technology, such as InfiniBand or Gigabit Ethernet. To enable clients to access a node, the node must be connected to the external Ethernet network. Redundant internal or external networks may be used for high availability.

## Network File Sharing Access Protocols

Different methods can be used to access files on a NAS system. The most common methods are:

### CIFS/SMB

Common Internet File System (CIFS) is a client/server application protocol that enables client programs to make requests for files and services on remote computers over TCP/IP. It is a non-proprietary version of the Microsoft Windows Server Message Block (SMB) protocol.

The CIFS protocol enables remote clients to gain access to files on a server. CIFS enables file sharing with other clients by using special locks. CIFS provides the following features to ensure data integrity:

- It uses file and record locking to prevent users from overwriting the work of another user on a file or a record.
- It supports fault tolerance and can automatically restore connections and reopen files that were open prior to an interruption.

Moreover, CIFS is a stateful protocol because the CIFS server maintains connection information regarding every connected client.

Users refer to remote file systems with an easy-to-use file-naming scheme:  
\\server\\share or \\servername.domain.suffix\\share.

### NFS

Network File System (NFS) is a client/server protocol for file sharing that is commonly used on UNIX systems. NFS was originally based on the connectionless User Datagram Protocol (UDP). It uses a machine-independent model to represent user data. It also uses Remote Procedure Call (RPC) for interprocess communication between two computers.

The NFS protocol provides a set of RPCs to access a remote file system for the following operations:

- Searching files and directories.
- Opening, reading, writing to, and closing a file.

- Changing file attributes.
- Modifying file links and directories.

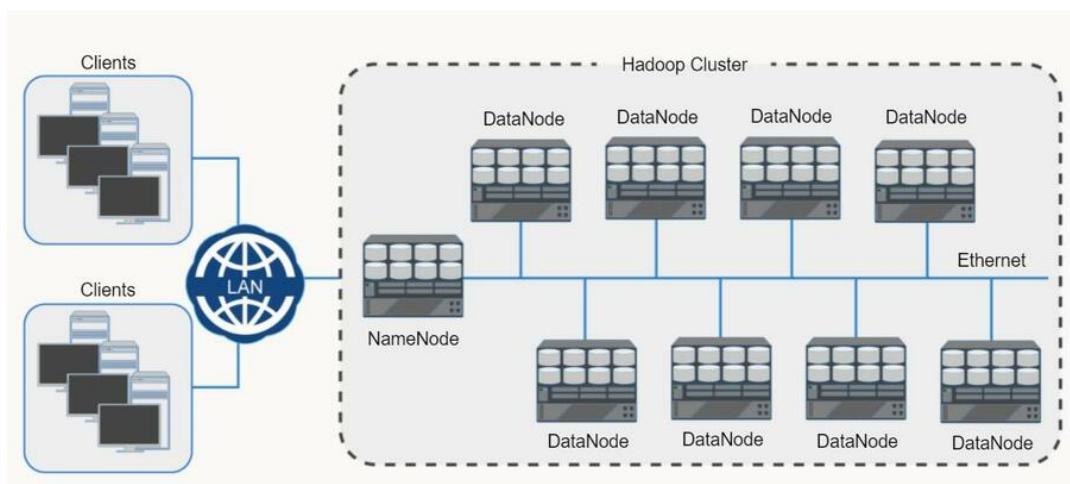
NFS creates a connection between the client and the remote system to transfer data.

## HDFS

Hadoop Distributed File System (HDFS) is supported by many of the scale-out NAS vendors. HDFS requires programmatic access because the file system cannot be mounted. All HDFS communication is layered on top of the TCP/IP protocol. HDFS has a primary/secondary architecture. An HDFS cluster consists of a single Name Node that acts as a master server.

This cluster has in-memory maps of every file, file locations as well as all the blocks within the file and which DataNodes they reside on. The NameNode is responsible for managing the file system namespace and controlling the access to the files by clients. DataNodes act as slaves that serve read/write requests and perform block creation, deletion, and replication as directed by the NameNode.

- A file system that spans multiple nodes in a cluster and enables user data to be stored in files.
- Presents a traditional hierarchical file organization so that users or applications can manipulate (create, rename, move, or remove) files and directories.
- Presents a streaming interface to run any application of choice using the MapReduce framework.



### FTP

- FTP is a client/server protocol that enables data transfer over an IP network.
- An FTP server and an FTP client communicate with each other using TCP as the transport protocol.
- FTP uses a set of commands and arguments to log in to the remote FTP client to access, manipulate, and transfer shared files and file metadata.

### S3

Amazon S3 is a service by Amazon Web Services (AWS) that provides *cloud-based* file sharing through an AWS web service interface. Among other services, S3 can perform the function of a networked file server, and file system. The S3 service offers tiered data storage, including long-term archive storage.

- Amazon S3 uses an Internet web services interface to store and share files over the Internet.

- Amazon S3 is a REST<sup>49</sup> service. Files that are stored in the user cloud space S3 instance are accessed over the Internet by issuing requests using the REST API<sup>50</sup>.
- Amazon S3 includes a file gateway that supports a file-level user interface.
  - The file gateway provides access to data in S3 as files or file system share mount points.
  - User files are stored and retrieved using the standard CIFS/SMB and NFS protocols.

---

<sup>49</sup> REST stands for Representational State Transfer. REST specifies a consistent architecture used to access and store data over the Internet. Commands such as GET, POST, PUT and DELETE are used in a client/server model to access, modify, transfer and store data.

<sup>50</sup> An API, or application programming interface, is a set of rules that define how applications or devices can connect and communicate. Typically, applications use APIs built into devices or systems to automate control and data transfer. A REST API is a specific API that conforms to the design architecture of REST. REST APIs communicate via HTTP to perform standard operations, such as file access, and read or write commands. S3 has a REST API front-end that accepts, and processes REST-based file access commands, and transfer requests.

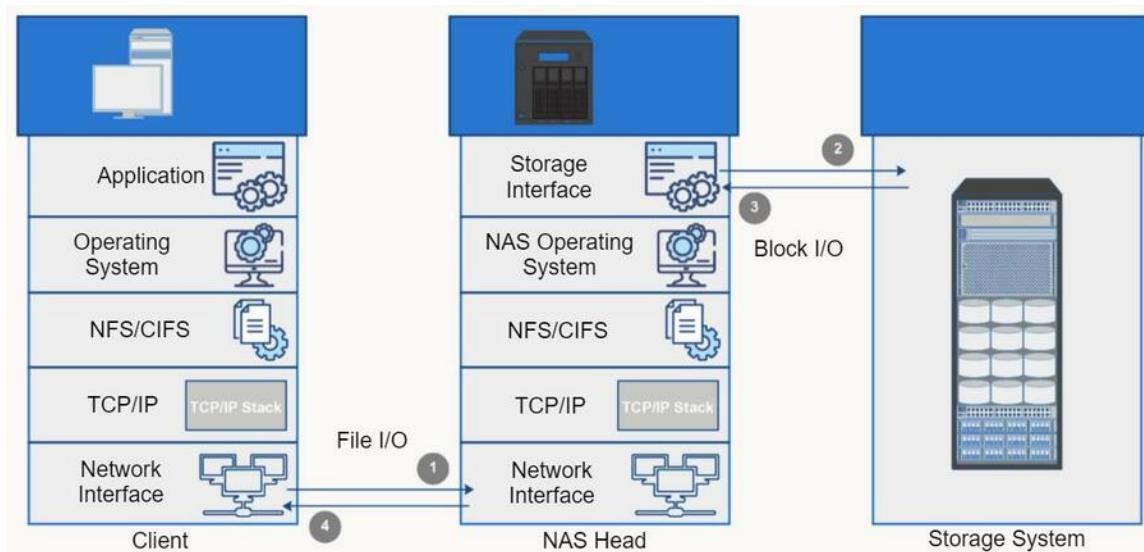
### NAS I/O Operation

Network file I/O operations differ between scale-up and scale-out NAS configurations.

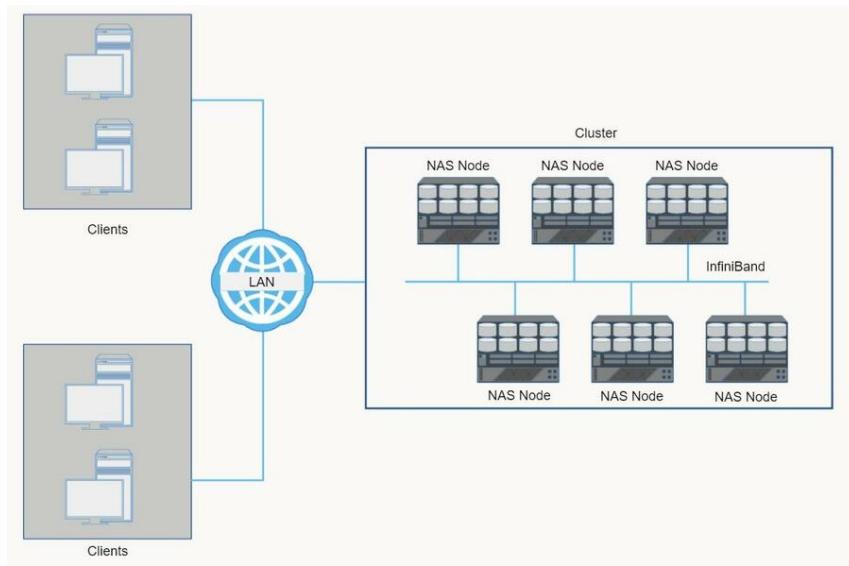
#### Scale-Up NAS I/O Operation

The figure illustrates an I/O operation in a scale-up NAS system. The process of handling read/write requests in a scale-up NAS environment is as follows:

1. The requestor (client) packages an I/O request into TCP/IP and forwards it through the network stack. The NAS system receives this request from the network.
2. The NAS system converts the I/O request into an appropriate physical storage request, which is a block-level I/O. This system then performs the operation on the physical storage.
3. When the NAS system receives data from the storage, it processes and repackages the data into an appropriate file protocol response.
4. The NAS system packages this response into TCP/IP again and forwards it to the client through the network.



## Scale-Out NAS I/O Operation



The figure illustrates I/O operation in a scale-out NAS system. A scale-out NAS consists of multiple NAS nodes and each of these nodes has the functionality similar to a NameNode or a DataNode. In some proprietary scale-out NAS implementations, each node may function as both a NameNode and DataNode, typically to provide Hadoop integration. All the NAS nodes in scale-out NAS are clustered.

Write Operation	Read Operation
<ol style="list-style-type: none"> <li>1. Client sends a file to the NAS.</li> <li>2. Node to which the client is connected receives the file.</li> <li>3. File is striped across the nodes.</li> </ol>	<ol style="list-style-type: none"> <li>1. Client requests a file.</li> <li>2. Node to which the client is connected receives the request.</li> <li>3. The node retrieves and rebuilds the file and gives it to the client.</li> </ol>

### Notes:

New nodes can be added as required. As new nodes are added, the file system grows dynamically and is evenly distributed to each node. As the client sends a file to store to the NAS system, the file is evenly striped across the nodes.

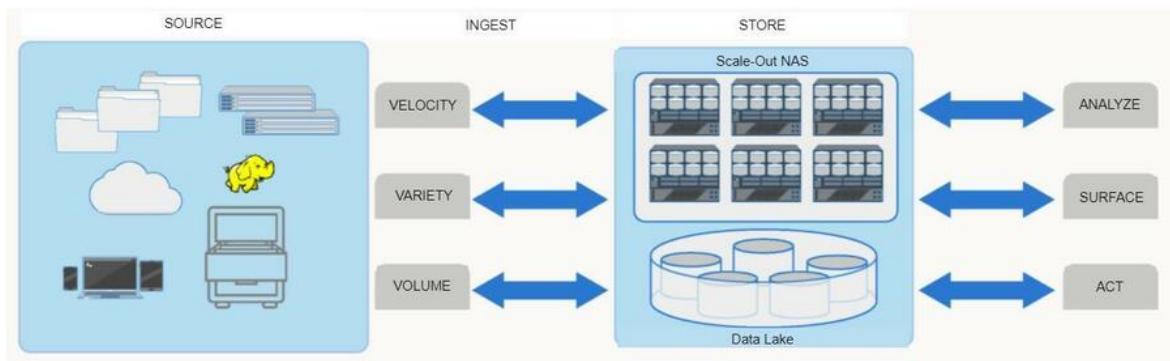
## File-Based Storage Systems

When a client writes data, even though that client is connected to only one node, the write operation occurs in multiple nodes in the cluster. This operation is also true for read operations.

A client is connected to only one node at a time. However, when that client requests a file from the cluster, the node to which the client is connected don't have the entire file locally on its drives. The node to which the client is connected retrieves and rebuilds the file using the back-end InfiniBand network.

## Use-Case for Scale-Out NAS: Data Lake

The data lake represents a change from the linear data flow model. As data increases in value, enterprise-wide data storage is transformed into a hub for data ingestion and consumption systems. This data hub enables enterprises to bring analytics to data and avoid expensive cost of multiple systems, storage, and time for ingestion and analysis.



The scale-out data lake:

- Accepts data from various sources like file shares, archives, web applications, devices, and the cloud.
- Enables data access for uses from conventional purposes to mobile, analytics, and cloud applications.
- Scales to meet the demands of consolidation and growth as technology evolves.
- Provides a tiering capability that enables organizations to manage costs without setting up specialized infrastructures.

### Notes:

By limiting the number of parallel, linear data flows. The enterprises can:

- Consolidate vast amounts of their data into a single store, a data lake, through a native and simple ingestion process.
- Perform analytics on the data to provide detailed insight.

## File-Based Storage Systems

- Actions can be taken based on this insight in an iterative manner.
- Eliminate the cost of having discrete silos or islands of information spread across the enterprises.

Scale-out NAS has the ability to provide the storage platform to this data lake. The scale-out NAS enhances this paradigm by providing scaling capabilities in terms of capacity, performance, security, and protection.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. What is a deficiency of using general-purpose servers for network file sharing?
  - a. File system incompatibilities when sharing files with clients that use different operating systems.
  - b. File system incompatibilities when sharing files with clients that are virtual machines.
  - c. File system incompatibilities when sharing files with clients that also serve files.
  - d. File system incompatibilities when sharing files with clients that use the S3 or HDFS protocols.

## Object-Based Storage Systems

## Drivers for Object-Based Storage

These are the key drivers for object-based storage adoption:

- Amount of data created annually is growing exponentially and more than 90% of data generated is unstructured.
  - Rapid adoption of third platform technologies leads to significant growth of data.
  - Longer data retention due to regulatory compliance also leads to data growth.
- Data must be instantly accessible through a variety of devices from anywhere in the world.
- Traditional storage solutions are inefficient in managing this data and in handling the growth.

### Notes:

In addition to increasing amounts of data, there has also been a significant shift in how people want, and expect to access data. The rising adoption rate of smartphones, tablets, and other mobile devices, combined with increasing acceptance of them in enterprise workplaces, has resulted in an expectation for on-demand access to data from anywhere, and on any type device.

Traditional storage solutions such as NAS, which is a dominant solution for storing unstructured data, are limited:

- Cannot scale to the capacities required or provide universal access across geographically dispersed locations.
- Data growth adds high overhead to the NAS in terms of managing large number of permission and nested directories.
  - File systems require more management as they scale and are limited in size.
  - Performance degrades as the NAS file system size increases. Increasing file system metadata capacity, a requirement of many new applications, is also limited.

## Object-Based Storage Systems

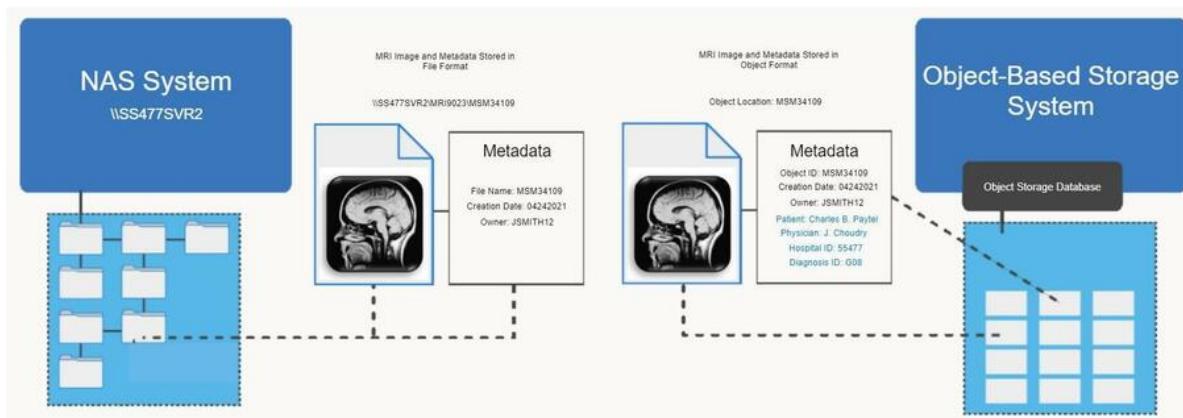
Object-based storage systems meet these challenges, and can better help to manage data growth at lower cost. Object-based storage provides extended metadata capabilities, and is highly scalable to keep up with rapidly growing data storage, and user access demands.

### What is an Object in Object-Based Storage?

An object is the fundamental unit of object-based storage.

Most object-based storage systems support API integration with software-defined data center and cloud environments.

- Objects contains user data, related metadata, and user defined attributes of data, such as retention, access pattern, and others.
  - Object metadata or attributes are used to optimize search, retention policies, and automated deletion of objects.
- Each object is identified by a unique object ID. The object ID allows access to objects without specifying the storage location.
  - The object ID is generated applying specialized algorithms to the data. This fingerprinting process guarantees unique object identification. Any changes to the object data results in a new object ID.
- An object storage database is used to track where objects and metadata are stored. For retrieval, the database uses the object ID to access the storage location records for the object and its metadata.

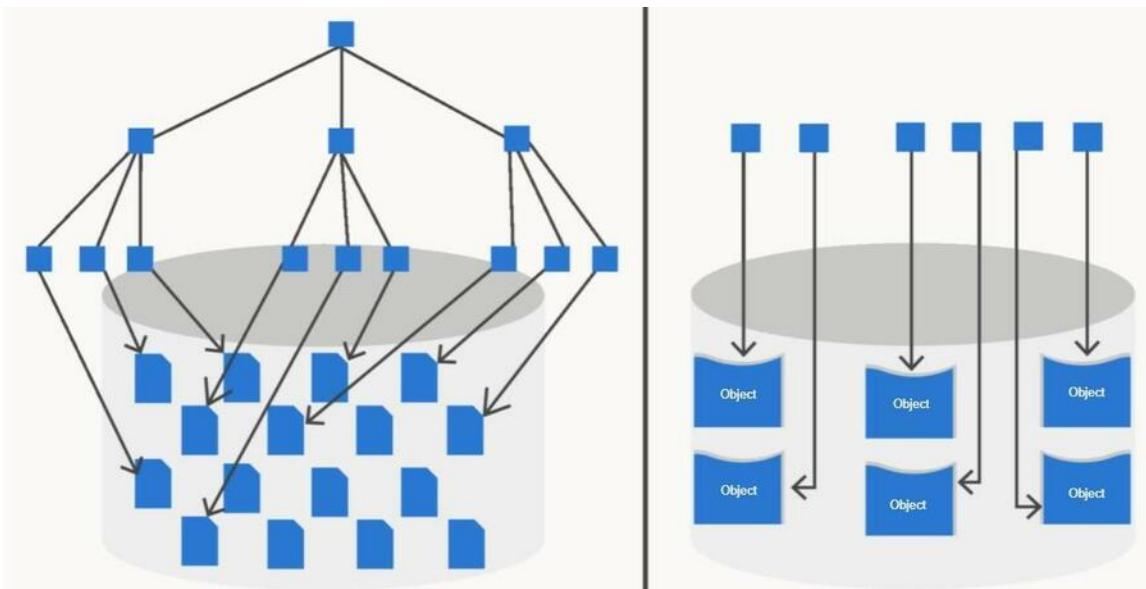


*Instead of storing data in a hierarchical structure of folders and files, object data is stored across a logically flat data repository.*

## Hierarchical File System Vs. Flat Address Space

An object storage device (OSD) stores data using a flat address space where objects exist at the same level, and one object cannot be placed inside another object. Therefore, there is no hierarchy of directories and files, and billions of objects can be stored in a single namespace.

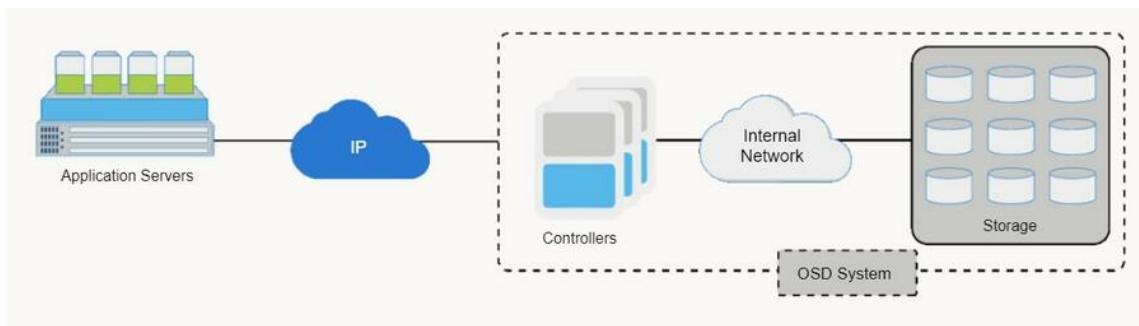
- Hierarchical file system organizes data in the form of files/directories
  - Limits the number of files that can be stored
- OSD uses a non-hierarchical, flat address space that enables storing large number of objects without having to maintain an absolute path to each object.
  - Enables the OSD to meet the scale-out storage indexing requirements of cloud computing, big data, and data analytics environments.



*The image on the left shows indexed data stored in a hierarchical file system. On the right is an example of data stored in a flat, non-hierarchical address space*

### Components of Object-Based Storage Device

The OSD system is composed of one or more controllers. A controller is a server that runs the OSD operating environment and provides services to store, retrieve, and manage data in the system. Typically OSD controllers use inexpensive x86-based servers. Each controller provides both compute and storage resources. OSD systems scale linearly in performance and capacity by adding controllers.



An OSD consists of controllers that connect to each other, and dedicated disk devices through an internal network. Client systems connect to the OSD over the IP network

OSD system typically comprises three key components:

- OSD controllers
- Internal network
- Storage

#### Notes:

The OSD controllers provide two key functions:

- **Metadata Service:** The metadata service is responsible for generating the object ID from the contents (may also include other attributes of data) of a file. It also maintains the mapping of the object IDs and the file system namespace. In some implementations, the metadata service runs inside an application server.
- **Storage Service:** The storage service manages a set of disks on which the user data is stored.

The OSD controllers connect to the storage via an internal network. The internal network provides inter-controller, and controller-to-storage connectivity. The application server accesses the controller to store and retrieve data over an

external network. OSD typically uses low-cost, high-density disk drives to store objects. As more capacity is required, more disk drives can be added to the system.

## Key Features of OSD Storage Systems

Object-based storage devices have these features:

Features	Description
Scale-out architecture	Provides linear scalability where nodes are independently added to the cluster to scale massively.
Multitenancy	Enables multiple applications/clients to be served from the same infrastructure
Metadata-driven policy	Intelligently drive data placement, protection, and data services based on the service requirements.
Global namespace	Abtracts storage from the application and provides a common view which is independent of location and making scaling seamless.
Flexible data access method	Supports REST/SOAP APIs for web/mobile access, and file sharing protocols (CIFS and NFS) for file service access.
Automated system management	Provides auto-configuring, auto-healing capabilities to reduce administrative complexity and downtime.
Data protection: Geo distribution	Object is protected using either replication or erasure coding technique and the copies are distributed across different locations.

### Notes:

Addition details for each OSD feature are:

- **Scale-out architecture:** Scalability has always been the most important characteristic of enterprise storage systems, since the rationale of consolidating storage assumes that the system can easily grow with aggregate demand. OSD is based on distributed scale-out architecture where each node in the cluster contributes with its resources to the total amount of space and performance.

Nodes are independently added to the cluster that provides massive scaling to support petabytes and even exabytes of capacity with billions of objects that make it suitable for cloud environment.

- **Multi-tenancy:** Enables multiple applications to be securely served from the same infrastructure. Each application is securely partitioned and data is neither co-mingled nor accessible by other tenants. This feature is ideal for businesses providing cloud services for multiple customers or departments within an enterprise.
- **Metadata-driven policy:** Metadata and policy-based information management capabilities combine to intelligently (automate) drive data placement, data protection, and other data services (compression, deduplication, retention, and deletion) based on the service requirements. For example, when an object is created, it is created on one node and subsequently copied to one or more additional nodes, depending on the policies in place. The nodes can be within the same data center or geographically dispersed.
- **Global namespace:** Another significant value of object storage is that it presents a single global namespace to the clients. A global namespace abstracts storage from the application and provides a common view, independent of location and making scaling seamless. This unburdens client applications from the need to keep track of where data is stored. The global namespace provides the ability to transparently spread data across storage systems for greater performance, load balancing, and non-disruptive operation. The global namespace is especially important when the infrastructure spans multiple sites and geographies.
- **Flexible data access method:** OSD supports REST/SOAP APIs for web/mobile access, and file sharing protocols (CIFS and NFS) for file service access. Some OSD storage systems support HDFS interface for big data analytics.
- **Automated system management:** OSD provides self-configuring and auto-healing capabilities to reduce administrative complexity and downtime. With respect to services or processes running in the OSD, there is no single point of failure. If one of the services goes down, and if the node becomes unavailable, or site becomes unavailable, there are redundant components and services that will facilitate normal operations.
- **Data protection:** The objects stored in an OSD are protected using two methods: replication and erasure coding. The replication provides data redundancy by creating an exact copy of an object. The replica requires the

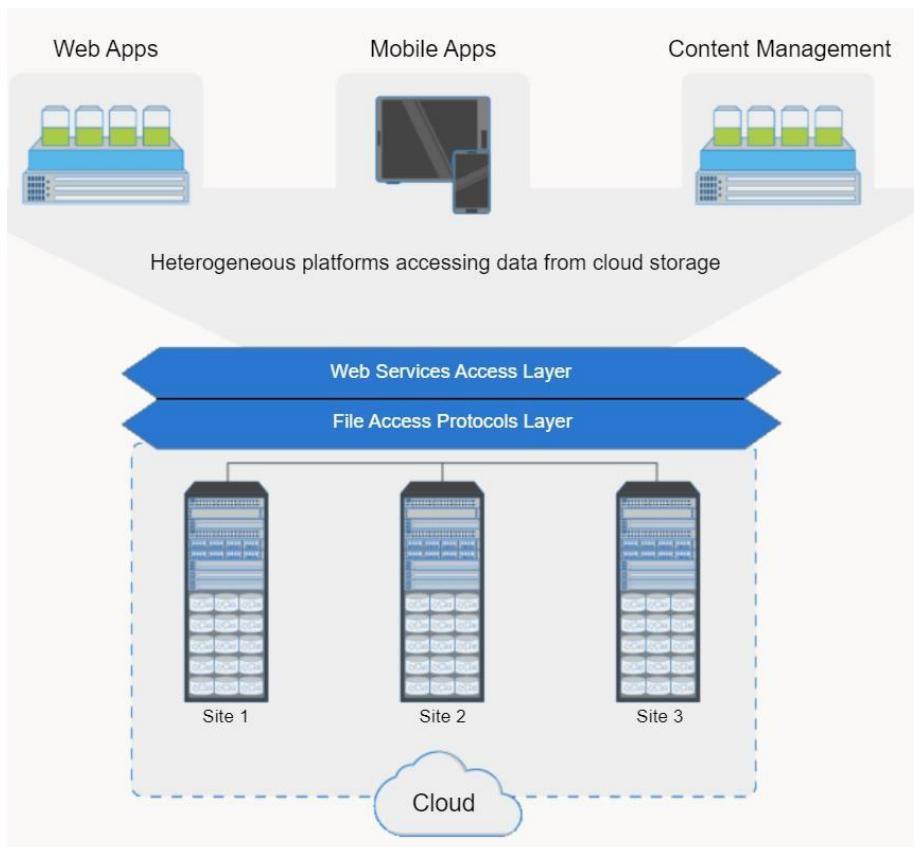
## Object-Based Storage Systems

same storage space as the source object. Based on the policy configured for the object, one or more replicas are created and distributed across different locations.

## Use Case: Cloud-Based Storage

OSD enables multi-tenancy, scalable cloud storage. Cloud storage provides geographic distribution of data with unified and universal access, policy-based data placement, and massive scalability. It also enables data access through web service or file access protocols and provides automated data protection to manage large amounts of data.

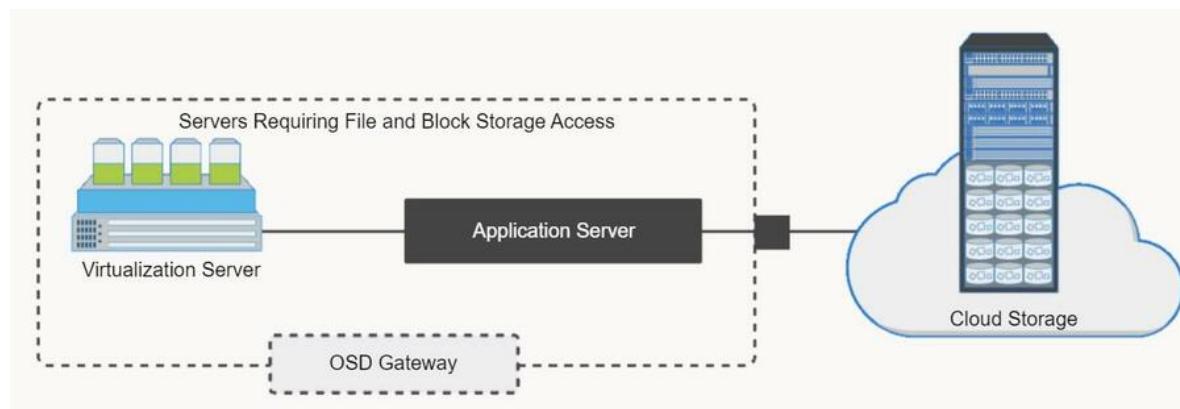
With the growing adoption of cloud computing, cloud service providers can leverage OSD to offer storage-as-a-service, backup-as-a-service, and archive-as-a-service to their consumers.



### Use Case: Cloud-based Object Storage Gateway

The lack of standardized cloud storage APIs has made the gateway a crucial component for cloud adoption. Service providers offer cloud-based object storage with interfaces such as REST or SOAP<sup>51</sup>. However, most business applications access storage resources through block-based iSCSI or FC interfaces, or file-based interfaces, such as NFS or CIFS.

OSD gateways provide a translation layer between iSCSI, FC, NFS, CIFS interfaces, and the cloud provider's REST API.



*The OSD gateway acts as a proxy to move file and block data to the cloud in response to REST API calls.*

The OSD gateway:

- Presents file and block-based storage interfaces to applications.

<sup>51</sup> SOAP is a messaging protocol for sending and receiving structured information within networked web services. SOAP uses the XML message format, and application layer protocols such as HTTP for transport. Where HTTP cannot be used, Simple Mail Transfer Protocol (SMTP) can be used for message transmission.

- Performs protocol conversion to send data directly to cloud storage.
- Encrypts the data before it transmits to the cloud storage.
- Supports deduplication and compression.
- Maintains a local cache to reduce latency for remote storage access.
- Provides a data management layer to determine what data to send to cloud storage or cache locally.
- Can be a physical appliance or a [virtual appliance](#) that runs gateway software.

Knowledge Check

## Knowledge Check

## Knowledge Check

1. What is true about how object data is stored in an OSD system?
  - a. Object data is stored in a logically flat data repository. Object data and metadata may be stored in different locations.
  - b. Object data is stored in a logically flat data repository. Object data and metadata are stored together.
  - c. Object data is stored on a logically hierarchical data repository. Object data and metadata are stored together.
  - d. Object data is stored in a logically hierarchical data repository. Object data and metadata may be stored in different locations.

## Knowledge Check

2. What is an attribute of an OSD gateway?
  - a. Presents file and block-based storage interfaces to applications.
  - b. Presents iSCSI and Fibre Channel-based storage interfaces to applications.
  - c. Presents HTTP and XML storage interfaces to applications.
  - d. Presents REST and SOAP-based storage interfaces to applications.

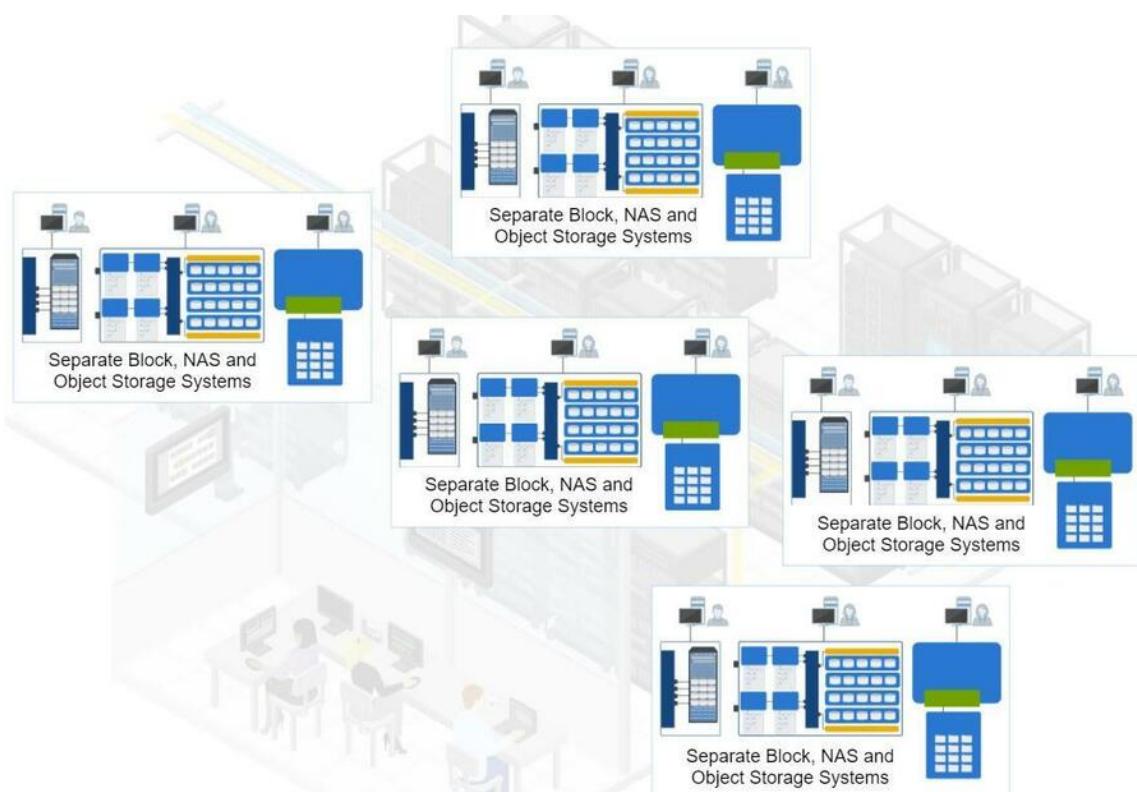
## Unified Storage Systems

## Unified Storage Systems

## Drivers for Unified Storage Systems

Midrange and large enterprise IT departments support a growing number of different applications and users. These applications and users require the IT department to provide and manage their storage capacity, scale, connectivity and protocol demands.

- The IT department must configure, administer, and manage an increasing number of separate block, file, and object-based storage systems.
- Providing increasing storage and services across separate systems is expensive and complex.
- IT personnel must master using different interfaces, software tools, and procedures to manage the storage infrastructure.

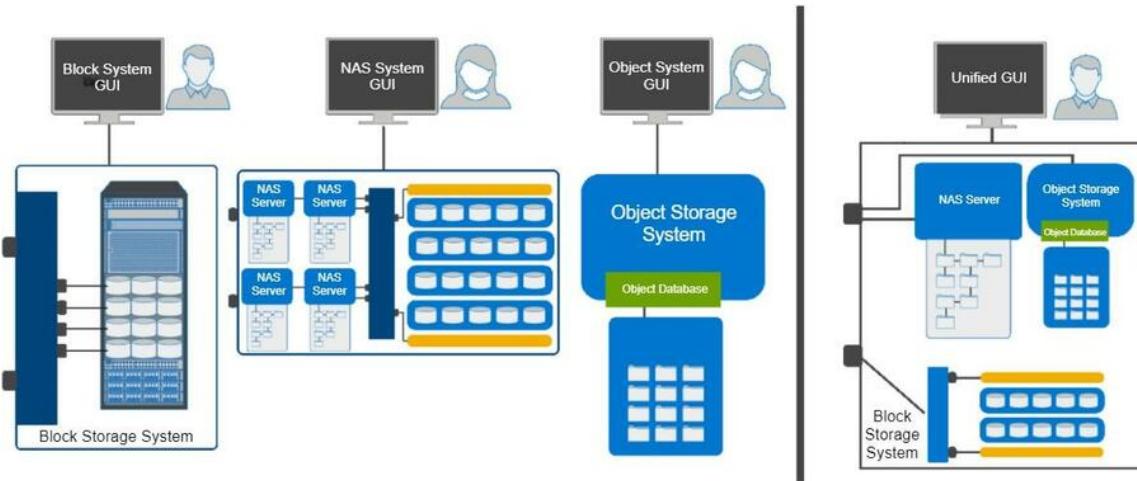


### Unified Storage System Architecture

Unified storage systems converge block, file, and object storage as well as configuration and management into a single platform. Unified storage lessens the administration and management impact of a growing storage infrastructure. Data storage and storage access remains transparent for applications and users.

Key benefits of unified storage systems are:

- Reduced number of separate storage systems.
  - Less environmental, acquisition, personnel, and administration and maintenance expenses.
- Reduced configuration, administration, and management complexity.
- Integration with a software-defined environment provides the right storage access for all users and applications.
- Increased utilization, with no stranded capacity. Unified storage eliminates the capacity utilization penalty.



*The image on the left shows separate block, file, and object storage systems. The image on the right shows them converged into a unified storage system*

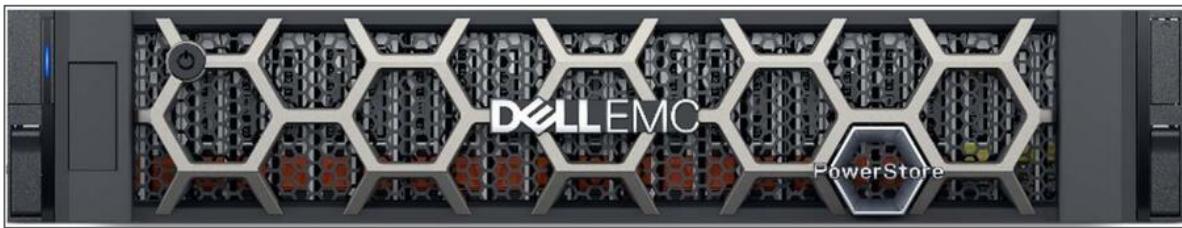
## Concepts in Practice

## Concepts in Practice

### Dell EMC PowerStore

Dell EMC PowerStore is a unified storage platform that stores and serves block and file data. Designed for growth, PowerStore can scale-up by adding storage capacity, and scale-out by adding storage controllers. The PowerStore platform provides:

- A scalable, single platform for block and file data storage and services.
- Active/active storage controllers with end-to-end NVMe storage connectivity.
- Flash or Storage Class Memory (SCM) internal storage devices.
- Integrated data optimization and protection services.



### Dell EMC PowerMax Series

Dell EMC PowerMax is a unified storage platform that stores and serves block and file data. Designed for growth, PowerMax can scale-up by adding storage capacity, and scale-out by adding storage controllers.

The PowerMax storage architecture offers:

- Up to 15M IOPS, 350 GB/s throughput (187 K IOPS per rack unit).
- Active/active storage controllers with end-to-end NVMe storage connectivity.
- Automated I/O recognition and data placement across NAND flash and SCM media to maximize performance with no management overhead.
- End to end efficient data encryption, and FIPS 140-2 validated Data at Rest Encryption.
- Integrated data optimization and protection services.



## Dell EMC PowerScale

PowerScale are scale-out NAS products that are based on the OneFS operating environment. Available as all-flash, hybrid and archive models, they achieve high scalability by pooling multiple nodes into a clustered NAS system that can store petabytes of file data. OneFS creates a single file system that spans across all nodes in a PowerScale cluster. These NAS products are optimized for file sharing and object data storage.

OneFS creates a single file system that spans across all nodes in a PowerScale cluster.

- Protocols: SMB (1, 2, 2.1, 3.x), NFS (v3, v4.0), FTP, SFTP, FTPS, S3, HDFS, HTTP.
- Scalability per file system namespace is 66 PB.

## Concepts in Practice

- Integrated data optimization and protection services.
- Scalability per cluster: 252 Nodes.



## Dell EMC ECS

Dell EMC ECS object scale storage appliances provide a hyperscale storage infrastructure that is designed to support modern applications. ECS provides a scalable, high availability architecture. It provides universal accessibility with support for object data, and the HDFS file system. The ECS platform provides:

- Hyperscale storage infrastructure.
- Universal accessibility with support for object and HDFS.
- Automated I/O recognition and data placement across NAND flash and SCM media to maximize performance with no management overhead.
- A single platform for web, mobile, big data, and social media applications.
- Data optimization and protection services.



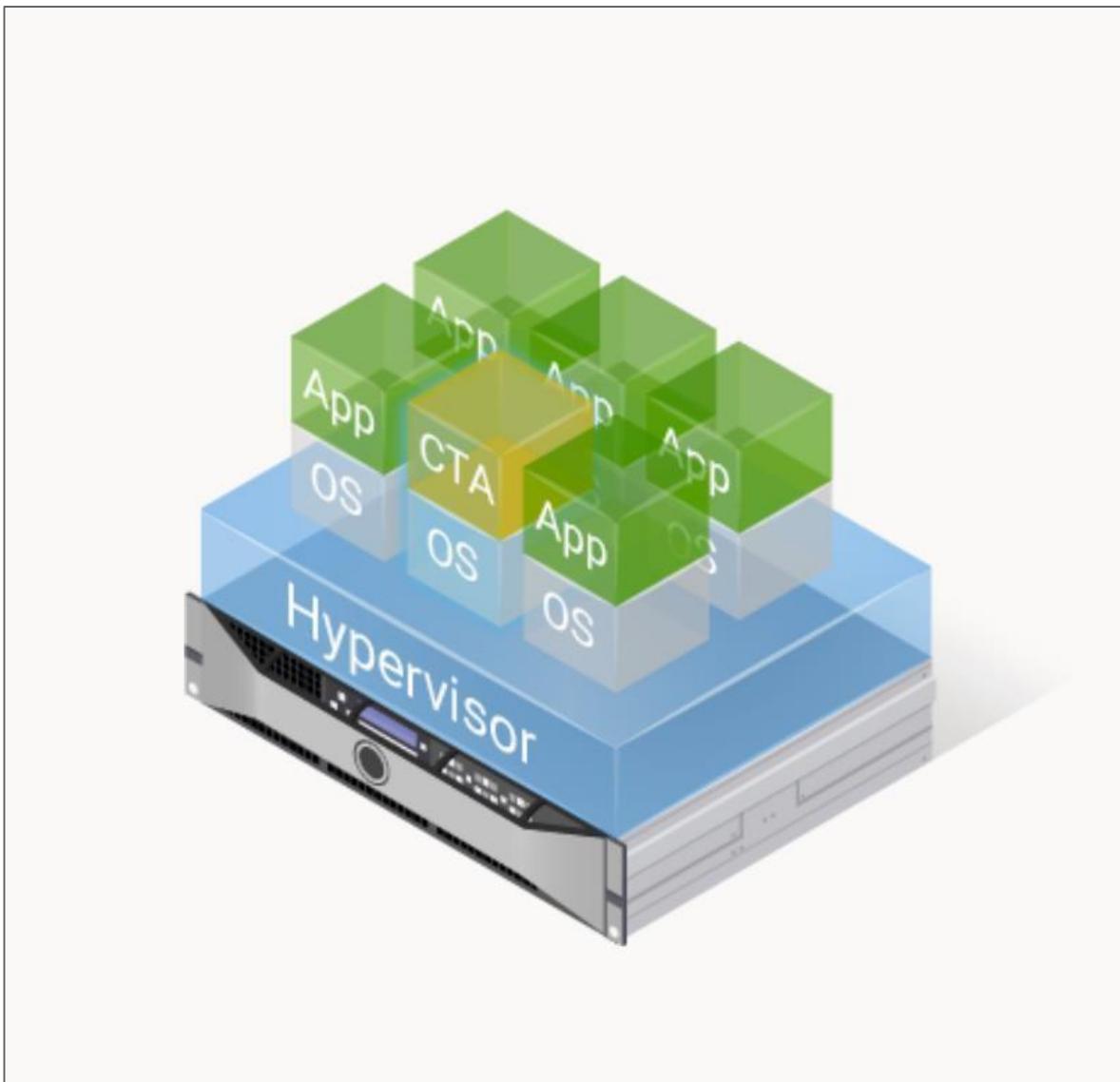
## Dell EMC Cloud Tiering Appliance

The Dell EMC Cloud Tiering Appliance (CTA) is packaged in the form of a virtual appliance. CTA is used to optimize primary file storage by automatically moving inactive files to secondary storage based on policies. Secondary storage can be lower-cost drives, such as SAS or SATA drives, or to other platforms, including public and private clouds. CTA can also provide block-level LUN data archiving for Dell EMC Unity storage systems.

Files that are moved, appear as if they are on primary storage. File tiering dramatically improves storage efficiency, and backup and restore time. File

archiving onto storage with WORM functionality can support additional business requirements such as compliance and retention.

- Tier or archive and recall file data.
- Automatically migrate files.
- Perform orphan file management.
- Simulate the potential effect of inactive file migration policies before starting the process.



## Storage Area Networking - FC SAN

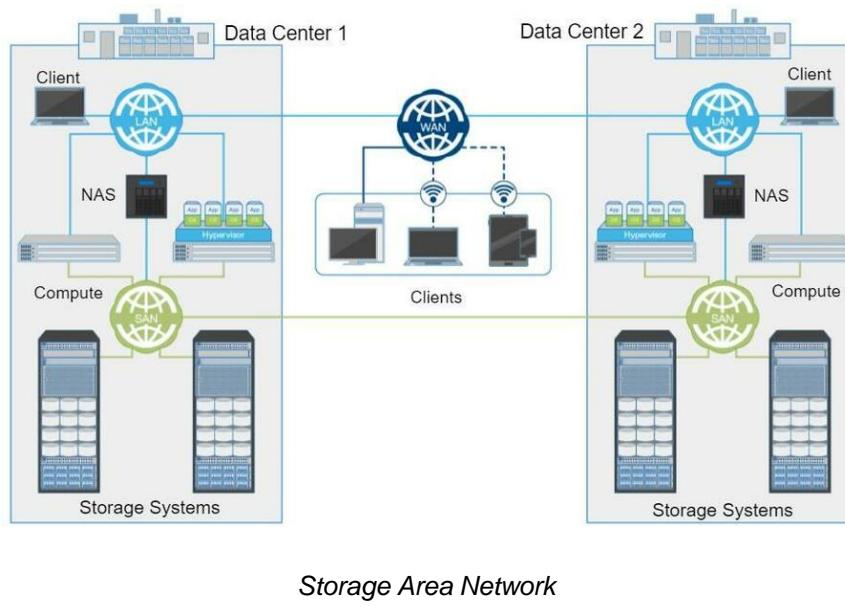
## Storage Area Network - FC SAN

## Introduction to SAN

## Business Needs and Technology Challenges

- An effective information management solution must provide:
  - Just-in-time information to business users.
  - Flexible and resilient storage infrastructure.
- Information management challenges in DAS environment:
  - Explosive growth of information storage that remains isolated and underutilized.
  - Proliferation of new servers and applications.
  - Complexity in sharing storage resources across multiple servers.
  - High cost of managing information.
- Storage area network (SAN) addresses these challenges.

### SAN Overview



Storage Area Network

- Organizations of all sizes use Storage Area Networks (SANs) to increase storage utilization rates (that is multiple hosts accessing the storage devices), improve application performance and availability, and to heighten security and data protection capabilities.
- A SAN consolidates storage silos by interconnecting compute and storage systems, and uses high-speed, reliable communication protocols, such as Fibre Channel.

### Benefits of SAN

- Consolidates storage resources across multiple compute systems.
  - Improves utilization of storage resources.
  - Centralizes management.
- Enables connectivity across geographically dispersed locations.
  - Enables compute systems across locations to access shared data.
  - Enables replication of data between storage systems that reside in separate locations.
  - Facilitates remote backup of application data.

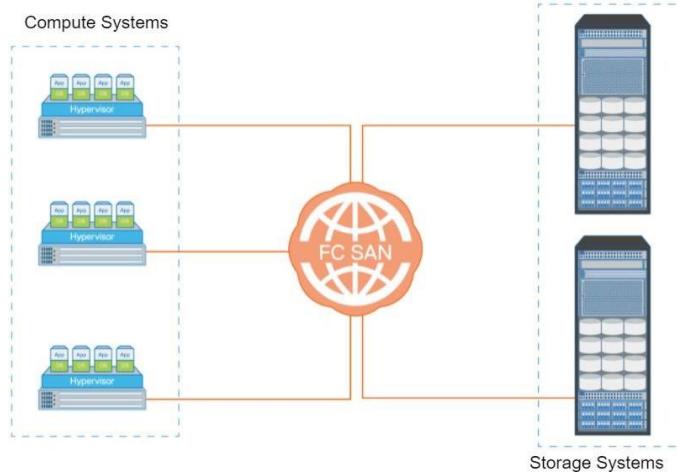
## Knowledge Check

## Knowledge Check

1. Which is the key benefit of SAN?
  - a. Eliminates the need to have HBAs on compute systems
  - b. Reduces the network bandwidth requirements while replicating data across storage systems
  - c. Allows to move from CAPEX to OPEX
  - d. Improves the utilization of storage resources

## Fibre Channel SAN

## FC SAN Overview



- A SAN that uses FC protocol for communication.
- FC protocol (FCP) is used to transport data, commands, and status information between the compute systems and the storage systems.
- FC is a high-speed network technology that runs on high-speed optical fiber cables and serial copper cables.
- FC speeds commonly run at 1, 2, 4, 8, 16, 32, 64, and 128 Gb/s.
- Provides high scalability.



**Fan-out** ratio is the ratio defined between a single port on a storage device and the total number of servers that are attached to it. A four-server connection to a single storage port results in a fan-out ratio of 4. If the fan-out ratio is high and the storage array becomes overloaded, then application performance will go down. **Fan-in** specifies accessibility of a host port to storage ports on multiple arrays.

## FC SAN Components

The key FC SAN components are network adapters, cables, and interconnecting devices.

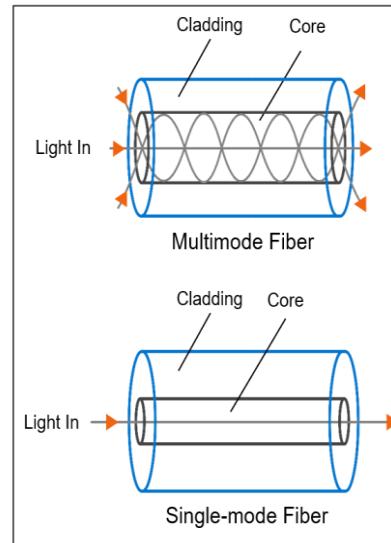
### Network Adapters

- In an FC SAN, the end devices, such as compute systems and storage systems are all referred to as nodes.
- Each node is a source or destination of FC frames. Each node requires one or more network adapters to provide a physical interface for communicating with other nodes.
- Examples of network adapters are FC host bus adapters (HBAs) and storage system front-end adapters.



### Cables

- FC SAN implementations primarily use optical fiber cabling.
- Copper cables may be used for shorter distances because it provides acceptable signal-to-noise ratio for distances up to 30 meters.
- Optical fiber cables carry data in the form of light. There are two types of optical cables: Multimode<sup>52</sup> and single-mode<sup>53</sup>.



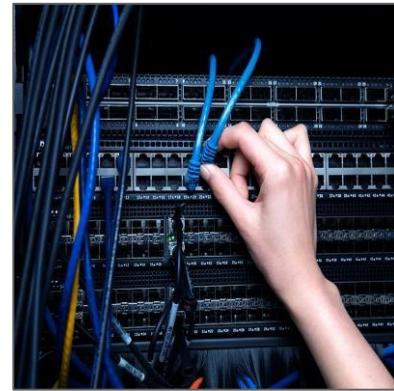
---

<sup>52</sup> Multimode fiber (MMF) cable carries multiple beams of light that is projected at different angles simultaneously onto the core of the cable. In an MMF transmission, multiple light beams traveling inside the cable tend to disperse and collide. This collision weakens the signal strength after it travels a certain distance – a process that is known as modal dispersion.

<sup>53</sup> Single-mode fiber (SMF) carries a single ray of light that is projected at the center of the core. The small core and the single light wave help to limit modal dispersion. Single-mode provides minimum signal attenuation over maximum distance (up to 10 km). A single-mode cable is used for long-distance cable runs, and the distance usually depends on the power of the laser at the transmitter and the sensitivity of the receiver.

## Interconnecting Devices

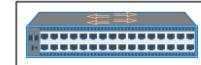
- The commonly used interconnecting devices in FC SANs are FC hubs, FC switches, and FC directors.



## FC Network Interconnecting Devices

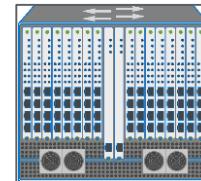
### FC Switches

- Each node has a dedicated communication path.
- Provides a fixed port count — active or unused.
- Active ports can be scaled-up non-disruptively.
- Some components are redundant and hot-swappable.

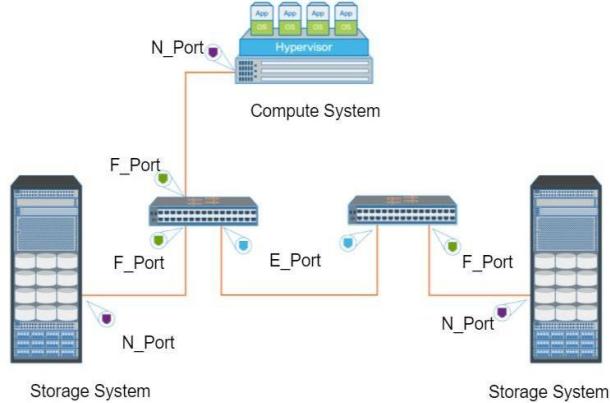


### FC Director

- High-end switches with a higher port count.
- Has a modular architecture.
- Port count is scaled-up by inserting line cards/blades.
- All key components are redundant and hot-swappable.



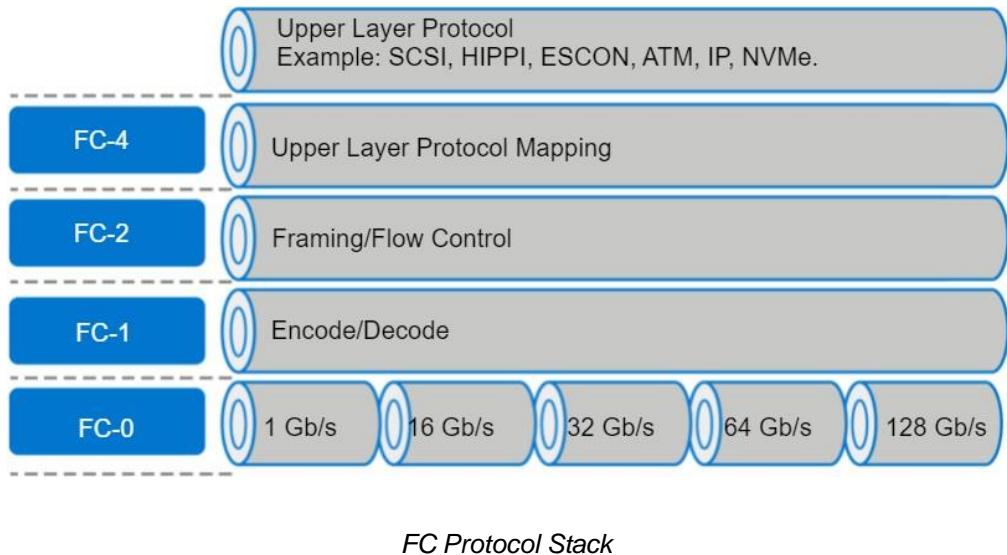
## FC SAN Device Port Types



*FC SAN Device Port Types*

Port	Description
N_Port	An end point in the fabric. This port is also known as the node port. Typically, it is a compute system port (FC HBA port) or a storage system port that is connected to a switch in a switched fabric.
E_Port	A port that forms the connection between two FC switches. This port is also known as the expansion port. The E_Port on an FC switch connects to the E_Port of another FC switch in the fabric ISLs.
F_Port	A port on a switch that connects an N_Port. It is also known as a fabric port.
G_Port	A generic port on a switch that can operate as an E_Port or an F_Port and determines its functionality automatically during initialization.

## FC SAN Protocol Stack



FC Layer	Function	Features Specified by FC Layer
FC-4	Mapping interface	Mapping upper layer protocol (for example SCSI) to lower FC layers
FC-3	Common services	Not implemented
FC-2	Routing, flow control	Frame structure, FC addressing, flow control
FC-1	Encode/decode	8b/10b or 64b/66b encoding, bit, and frame synchronization
FC-0	Physical layer	Media, cables, connector

### Notes:

**FC-4 Layer:** It is the uppermost layer in the FCP stack. This layer defines the application interfaces and the way Upper Layer Protocols (ULPs) are mapped to the lower FC layers. The FC standard defines several protocols that can operate on

the FC-4 layer. Some of the protocols include SCSI, High Performance Parallel Interface (HIPPI) Framing Protocol, ESCON, Asynchronous Transfer Mode (ATM), and IP.

**FC-2 Layer:** It provides FC addressing, structure, and organization of data (frames, sequences, and exchanges). It also defines fabric services, classes of service, flow control, and routing.

**FC-1 Layer:** It defines how data is encoded prior to transmission and decoded upon receipt. At the transmitter node, an 8-bit character is encoded into a 10-bit transmission character. This character is then transmitted to the receiver node. At the receiver node, the 10-bit character is passed to the FC-1 layer, which decodes the 10-bit character into the original 8-bit character. FC links, with a speed of 10 Gbps and above, use 64-bit to 66-bit encoding algorithm. This layer also defines the transmission words such as FC frame delimiters, which identify the start and the end of a frame and the primitive signals that indicate events at a transmitting port. In addition to these, the FC-1 layer performs link initialization and error recovery.

**FC-0 Layer:** It is the lowest layer in the FCP stack. This layer defines the physical interface, media, and transmission of bits. The FC-0 specification includes cables, connectors, and optical and electrical parameters for various data rates. The FC transmission can use both electrical and optical media.

## FC Frame

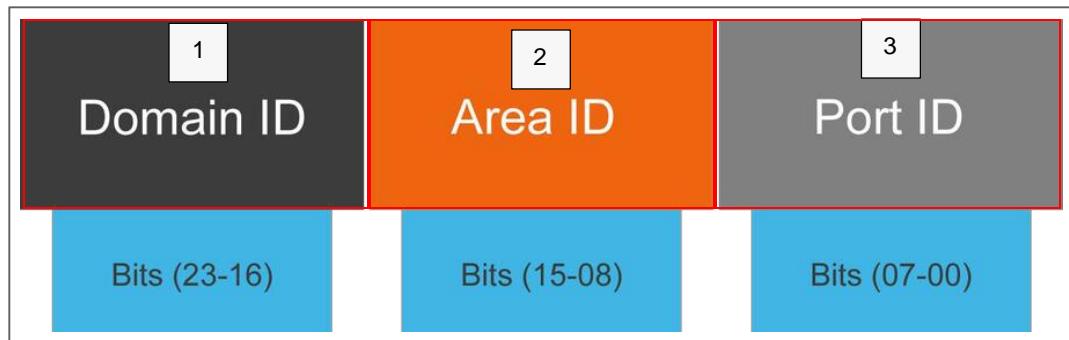


- A frame is the fundamental unit of data transfer at FC-2 layer.
- Consists of five parts: start of frame (SOF), frame header, data field, cyclic redundancy check (CRC), and end of frame (EOF).
  - **SOF and EOF:** Act as delimiters.
  - **Frame header:** Is 24 bytes long and contains addressing information for the frame.
  - **Data field:** Contains the data payload, up to 2,112 bytes of actual data—in most cases, the SCSI data.
  - **CRC:** Checksum facilitates error detection for the content of the frame. It verifies data integrity by checking whether the content of the frames was received correctly.

## FC Addressing in Switched Fabric

- FC address is assigned to node ports during fabric login.
  - Used for communication between nodes in a FC SAN
- Main purpose of an FC address is routing data through the fabric.
- FC address size is 24 bits.

***Click each highlighted block for more details.***



**1:** A domain ID is a unique number that is provided to each switch in the fabric.

**2:** The area ID is used to identify a group of switch ports that are used for connecting nodes.

**3:** The port ID identifies the port within the group.

## World Wide Name

- Unique 64-bit identifier.
- Static to node ports on an FC network.
  - Similar to MAC (Media Access Control) address of NIC (Network Interface Card).
  - The FC environment uses two types of WWNs: World Wide Node Name (WWNN) and World Wide Port Name (WWPN).
  - WWNN and WWPN are used to physically identify FC network adapters and node ports, respectively.

5	0	0	6	0	1	6	0	0	0	6	0	0	1	B	2
0101	0000	0000	0110	0000	0001	0110	0000	0000	0000	0110	0000	0000	0001	1011	0010
<small>Port Type: Company ID 24 Bits Model/Speed 32 Bits</small>															
<small>Reserve 12 Bits Company ID 24 Bits Company Specific 24 Bits</small>															
1	0	0	0	0	0	0	0	c	9	2	0	d	c	4	0

World Wide Name - Array (The top WWN is for an array port, and the bottom WWN is for a HBA)

## FC SAN: Additional Information



*Click [here](#) to understand about Fibre Channel storage networking technology*

Knowledge Check

## Knowledge Check

## Knowledge Check

1. Which characteristic describes an FC switch?
  - a. Each node has a dedicated communication path.
  - b. Nodes are connected in a logical loop.
  - c. Nodes share loop.
  - d. Provides limited connectivity and scalability.

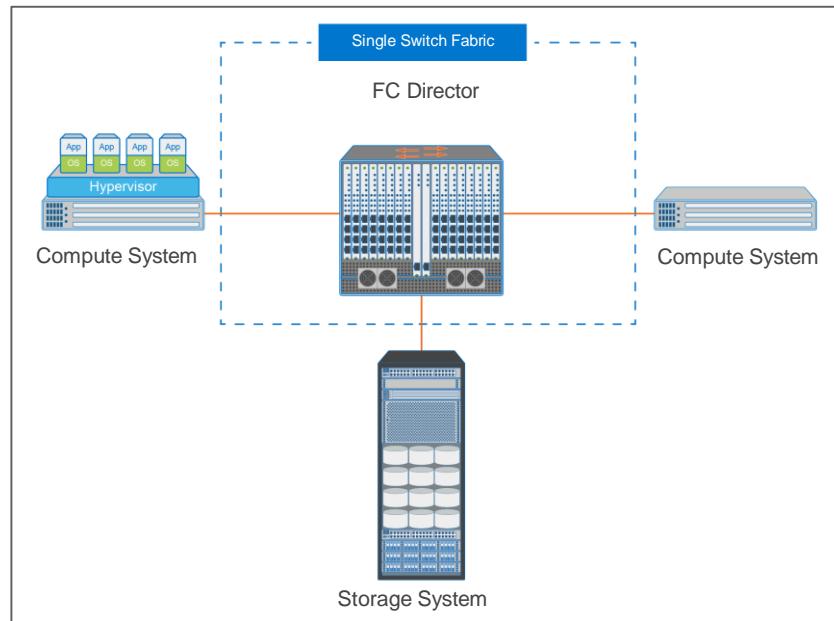
## FC SAN Topologies, Link Aggregation and Zoning

## FC SAN Topologies, Link Aggregation and Zoning

## FC SAN Topologies

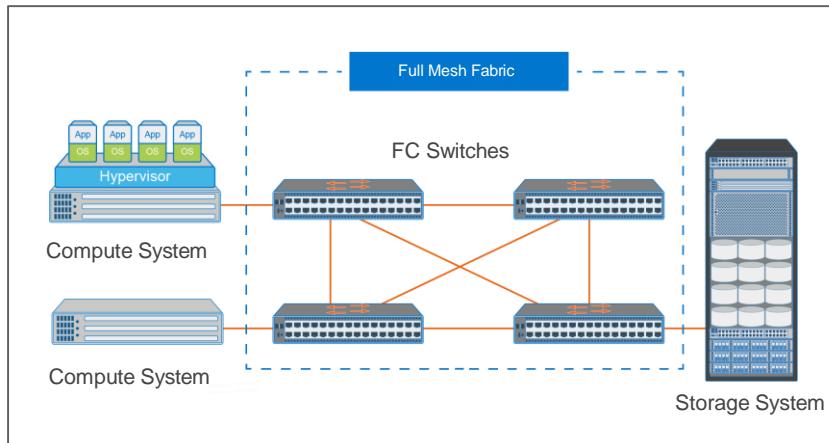
FC switches (including FC directors) may be connected to form various different fabric topologies.

### Single Switch Fabric Topology



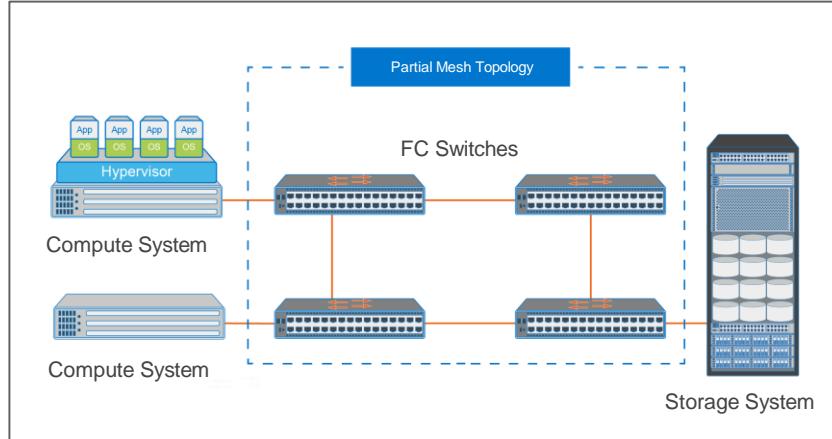
- Fabric consists of only a single switch.
- Both compute systems and storage systems connect to same switch.
- No ISLs are required for compute-to-storage traffic.
- Every switch port is usable for node connectivity.

### Full Mesh Topology



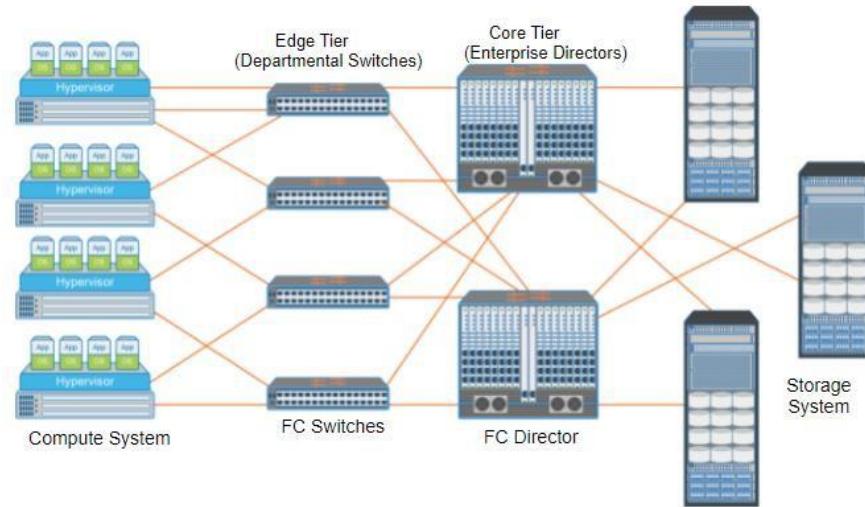
- Each switch is connected to every other switch.
- Maximum of one ISL is required
- Compute systems and storage systems can be connected to any switch.

### Partial Mesh Topology



- Not all the switches are connected to every other switch.
- Several ISLs may be required.

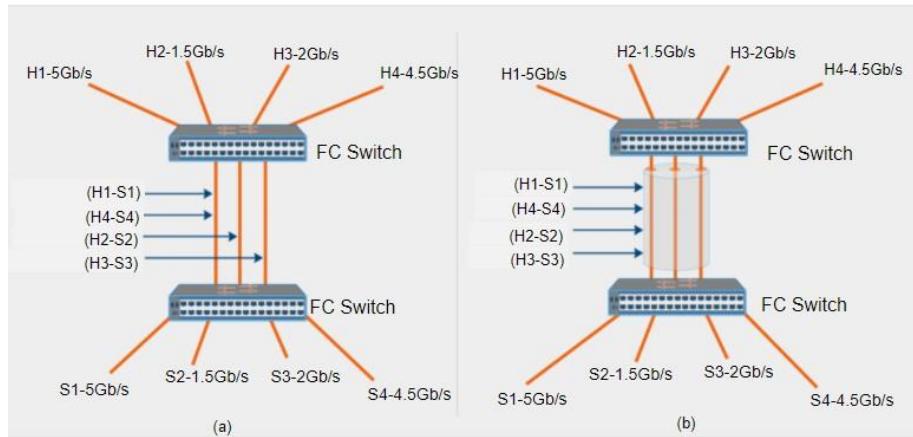
### Core-Edge Topology



- The edge tier is composed of departmental switches and offers an inexpensive approach to adding more compute systems in a fabric.
- The edge-tier switches are not connected to each other.
- Each switch at the edge tier is attached to a enterprise director at the core tier through ISLs.
- Compute systems that require high performance may be connected directly to the core tier and therefore avoid ISL delays.
- The core-edge topology increases connectivity within the FC SAN while conserving the overall port utilization.

## Link Aggregation

- Combines two or more parallel ISLs into a single logical ISL, called a port-channel, yielding higher throughput than a single ISL could provide.
- Distributes network traffic over ISLs, ensuring even ISL utilization.



(a) Without Link Aggregation and (b) With Link Aggregation

### Notes:

This image illustrates two examples.

The example here is based on an FC SAN infrastructure with no link aggregation enabled.

- Four HBA ports H1, H2, H3, and H4 have been configured to generate I/O activity to four storage system ports S1, S2, S3, and S4 respectively.
- The HBAs and the storage systems are connected to two separate FC switches with three ISLs between the switches.
- Let us assume that the bandwidth of each ISL is 8 Gb/s and the data transmission rate for the port-pairs {H1,S1}, {H2,S2}, {H3,S3}, and {H4,S4} are 5 Gb/s, 1.5 Gb/s, 2 Gb/s, and 4.5 Gb/s.

Without link aggregation, the fabric typically assigns a particular ISL for each of the port-pairs in a round-robin fashion. It is possible that port-pairs {H1,S1} and {H4,S4} are assigned to the same ISL in their respective routes. The other two ISLs are assigned to the port-pairs {H2,S2} and {H3,S3}. Two of the three ISLs are under-

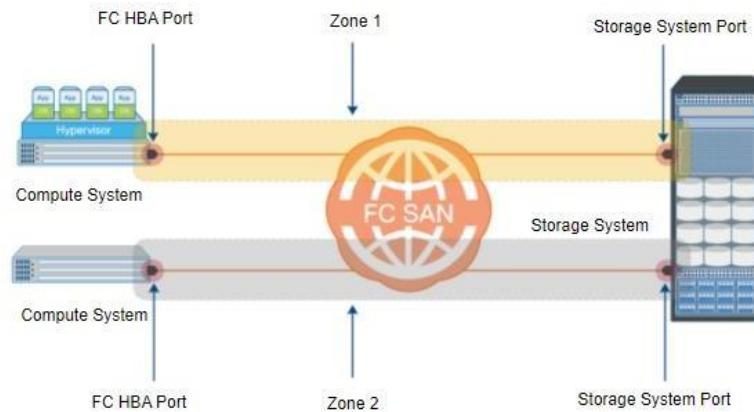
## FC SAN Topologies, Link Aggregation and Zoning

utilized, whereas the third ISL is saturated and becomes a performance bottleneck for the port-pairs assigned to it.

The example on the right has aggregated the three ISLs into a port-channel that provides throughput up to 24 Gb/s. Network traffic for all the port-pairs are distributed over the ISLs in the port-channel, which ensures even ISL utilization.

## FC SAN Zoning

A logical private path between node ports in a fabric.



- Each zone contains members (FC HBA and storage system ports).
- Provides security and restricts registered state change notification (RSCN) traffic.
- Provides access control by enabling only the members in the same zone to communicate with each other.

### Notes:

Zoning is a logical private path between node ports in a fabric. Whenever a change takes place in the name server database, the fabric controller sends a Registered State Change Notification (RSCN) to all the nodes impacted by the change. If zoning is not configured, the fabric controller sends the RSCN to all the nodes in the fabric. Involving the nodes that are not impacted by the change increases the amount of fabric-management traffic.

For a large fabric, the amount of FC traffic generated due to this process can be significant and might impact the compute-to-storage data traffic. Zoning helps to limit the number of RSCNs in a fabric. In the presence of zoning, a fabric sends the RSCN to only those nodes in a zone where the change has occurred.

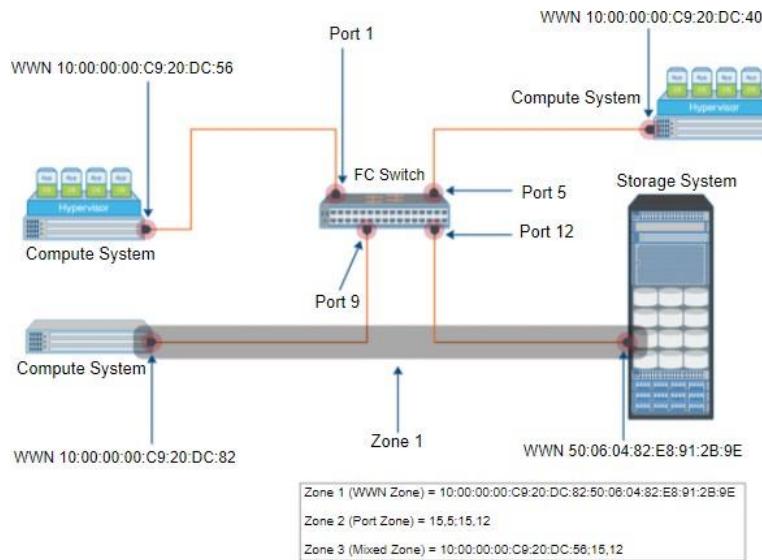
Zone members, zones, and zone sets form the hierarchy that is defined in the zoning process. A zone set is composed of a group of zones that can be activated

## FC SAN Topologies, Link Aggregation and Zoning

or deactivated as a single entity in a fabric. Multiple zone sets may be defined in a fabric, but only one zone set can be active at a time.

## FC SAN Zoning Types

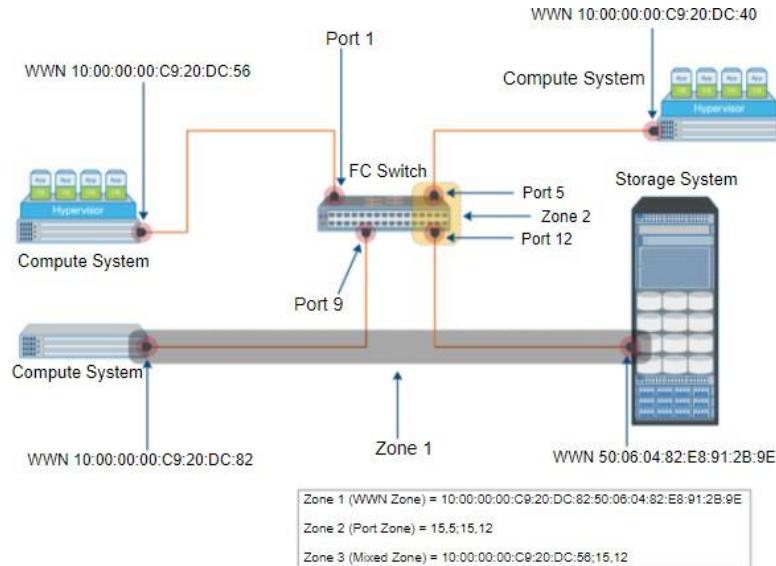
### WWN Zoning



Uses World Wide Names to define zones. The zone members are the unique WWN of the FC HBA and its targets (storage systems). A major advantage of WWN zoning is its flexibility.

## FC SAN Topologies, Link Aggregation and Zoning

### Port Zoning

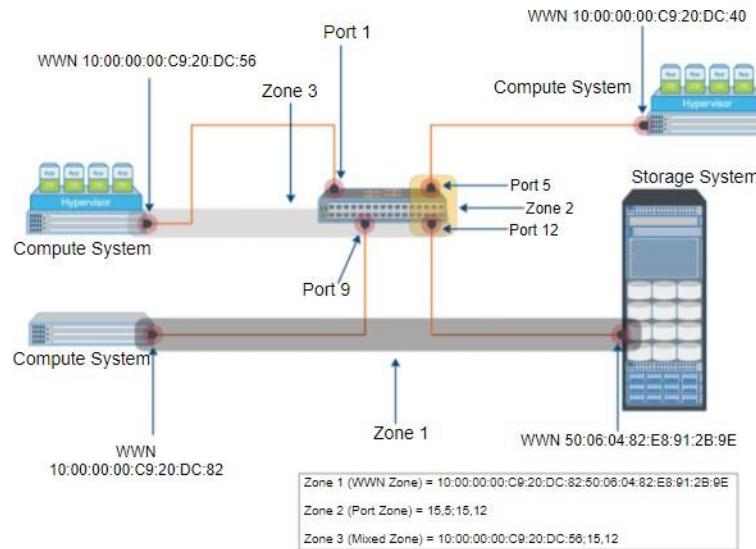


Uses the switch port ID to define zones. In port zoning, access is determined by the physical switch port to which a node is connected. The zone members are the port identifiers (switch domain ID and port number) to which FC HBA and its targets (storage systems) are connected.

### Mixed Zoning

Combines the qualities of both WWN zoning and port zoning. Using mixed zoning enables a specific node port to be tied to the WWN of another node.

## FC SAN Topologies, Link Aggregation and Zoning



### Notes:

**WWN Zoning** - If an administrator moves a node to another switch port in the fabric, the node maintains connectivity to its zone partners without having to modify the zone configuration. This functionality is possible because the WWN is static to the node port.

**Port Zoning** - If a node is moved to another switch port in the fabric, port zoning must be modified to enable the node, in its new port, to participate in its original zone. However, if an FC HBA or storage system port fails, an administrator has to replace the failed device without changing the zoning configuration.

## FC Fabric: Additional Information



Click [here](#) to understand about Fibre Channel fabric

## Knowledge Check

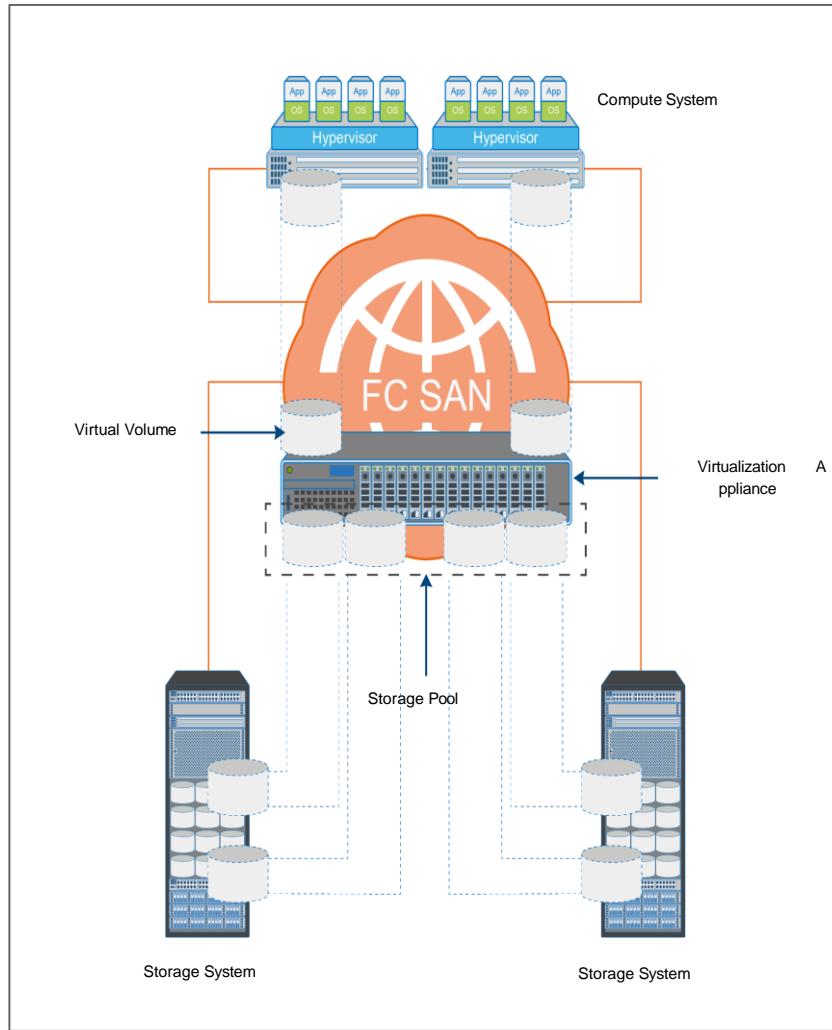
## Knowledge Check

### Knowledge Check

1. Which FC SAN zoning type is determined by the physical switch port to which the node is connected?
  - a. WWN zoning
  - b. WWN zoning and Port zoning
  - c. Mixed zoning
  - d. Port zoning

## SAN Virtualization

## Block-level Storage Virtualization



- Provides a virtualization layer in the SAN.
  - Abstracts block-based storage systems
  - Aggregates LUNs to create storage pools.
- Virtual volumes from a storage pool are assigned to compute systems.
  - Virtualization layer maps virtual volumes to LUNs
- Benefits:
  - Online expansion of virtual volumes.
  - Non-disruptive data migration.

**Notes:**

Block-level storage virtualization aggregates block storage devices (LUNs) and enables provisioning of virtual storage volumes, independent of the underlying physical storage. A virtualization layer, which exists at the SAN, abstracts the identity of block-based storage systems and creates a storage pool by aggregating LUNs from the storage systems.

Virtual volumes are created from the storage pool and assigned to the compute systems. Instead of being directed to the LUNs on the individual storage systems, the compute systems are directed to the virtual volumes provided by the virtualization layer. The virtualization layer maps the virtual volumes to the LUNs on the individual storage systems.

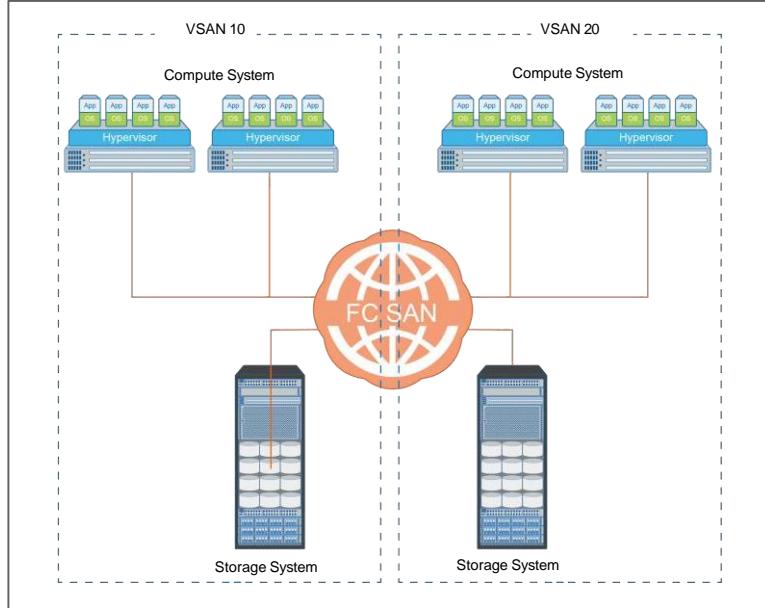
The compute systems remain unaware of the mapping operation and access the virtual volumes as if they were accessing the physical storage attached to them. Typically, the virtualization layer is managed via a dedicated virtualization appliance to which the compute systems and the storage systems are connected.

Block-level storage virtualization enables extending the virtual volumes non-disruptively to meet application's capacity scaling requirements. It also provides the advantage of non-disruptive data migration. In a traditional SAN environment, LUN migration from one storage system to another is an offline event.

After migration, the compute systems are updated to reflect the new storage system configuration. In other instances, processor cycles at the compute system were required to migrate data from one storage system to the other, especially in a multivendor environment.

With a block-level storage virtualization solution in place, the virtualization layer handles the migration of data, which enables LUNs to remain online and accessible while data is migrating. No physical changes are required because the compute system still points to the same virtual volume on the virtualization layer. However, the mapping information on the virtualization layer should be changed. These changes can be executed dynamically and are transparent to the end user.

### Virtual Fabric - VSAN



- VSAN enables a group of node ports to communicate with each other using a virtual topology that is defined on the physical SAN.
  - Multiple VSANs may be created on a single physical SAN.
  - Each VSAN behaves and is managed as an independent fabric.
  - Each VSAN has its own fabric services, configuration, and set of FC addresses.
  - Fabric-related configurations in one VSAN do not affect the traffic in another VSAN.
  - A VSAN may be extended across sites, enabling communication among a group of nodes, in either site with a common set of requirements.
- Improve SAN security, scalability, availability, and manageability.
- Facilitate an easy, flexible, and less expensive way to manage networks.
- For example, an IT administrator typically isolates the storage pools for multiple IT services by creating multiple VSANs on an FC SAN.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. What is a benefit of implementing VSANs?
  - a. Provides non-disruptive data backup
  - b. Improves network security
  - c. Aggregates LUNs across storage systems
  - d. Increases the performance of SAN switch by 2X

## Concepts in Practice

## Concepts in Practice

### Dell EMC Connectrix

Connectrix B-Series and Connectrix MDS Series switches offer a range of enterprise, departmental, edge switches and top-of-rack switches for small to large enterprise environments. All 32Gbs switches support FC-NVMe.

#### Features

 Fibre Channel connectivity of up to 64 gigabits per second and Gigabit Ethernet speeds up to 40 GbE.

 Scales from 8 to 128 ports per system.

 Uses redundant components and multipath deployment to ensure high availability and failover.

 Monitors your storage networking environment automatically with resilient networking features.



### DELL EMC PowerSwitch S4100-ON

The S4100-ON 10GbE switches comprise Dell Technologies latest disaggregated hardware and software data center networking solutions, providing state-of-the-art 100GbE uplinks, fibre channel connectivity and a broad range of functionalities.

The S4100-ON series are high-performance, multifunction, 1/10/25/40/50/100 GbE and 8/16/32G FC top-of-rack (ToR) switches purpose-built for applications in high-performance data center, cloud and computing environments.



## DELL EMC MXG610S Fibre Channel Switch

The Dell EMC Networking MXG610s 32G Fibre Channel IO Module for the PowerEdge MX7000 is the right choice for mission-critical applications accessing data on external storage.

- Provides industry-leading performance with the latest generation of Fibre Channel.
- Provides consolidated management for an agile management structure and simplified server and storage connectivity.
- Employs a responsive design which protects enterprise's infrastructure with inherent security and with non-disruptive upgrades to NVMe over Fibre Channel.
- Enables high-throughput, high-density, low-latency Fibre Channel IO Module purpose-built for the PowerEdge MX7000, optimized for flash storage and highly virtualized server environments.



## Dell EMC VPLEX

- Provides solution for block-level storage virtualization and data migration both within and across data centers.
- Provides the capability to mirror data of a virtual volume both within and across locations.

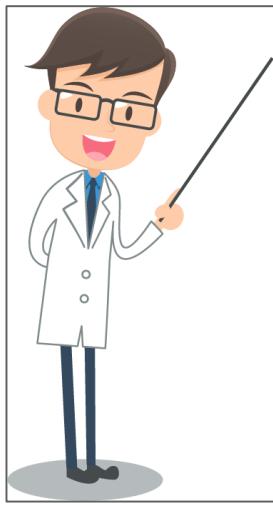
## Concepts in Practice

- VS6 engine with VPLEX for all-flash model provides the fastest and most scalable VPLEX solution for all-flash systems.
- Enables organizations to move cold data to inexpensive cloud storage.



## Exercise

## Exercise: FC SAN Topologies



### Scenario

- An organization's storage infrastructure includes three block-based storage systems.
- Storage systems are direct-attached to 45 compute systems.
- Compute systems are dual-attached to the storage systems.
- Each storage system has 32 front-end ports, which could support a maximum of 16 compute systems.
- Each storage system has the storage drive capacity to support a maximum of 32 compute systems.

### Challenges

- Organization requires an additional 45 compute systems to meet its growth requirements.
- Existing storage systems are poorly utilized.
- The addition of new compute systems require an addition of new storage systems.
- Organization wants to implement FC SAN to overcome the scalability and utilization challenges.
- Number of ISLs required for compute-to-storage traffic must be minimized to meet the performance requirement of applications.

### Deliverables

Given that 72-port FC switches are available for interconnectivity:

- Propose a fabric topology to address organization's challenges/requirements and justify your choice.
- Determine the minimum number of switches required in the fabric.

## Debrief

The recommended solution is core-edge topology:

- Provides higher scalability than mesh topology.
- Provides a maximum of one-hop/one-ISL storage access to all compute systems.
- Increases connectivity by conserving the overall switch port utilization.

The recommended configuration:

- Total number of compute system ports = 90 compute systems  $\times$  2 ports = 180 ports.
- Total number of storage system ports = 3 storage systems  $\times$  32 ports = 96 ports.
- Number of switches at the core = 96 storage system ports / 72 ports per switch  $\approx$  2 switches.
  - Core switches provide 144 ports of which 96 ports will be used for storage system connectivity.
  - Remaining 48 ports can be used for ISLs and future growth.
- Number of switches at the edge = 180 compute system ports / 72 ports per switch  $\approx$  3 switches.
  - Edge switches provide 216 ports of which 180 ports will be used for compute system connectivity.
  - Remaining 36 ports can be used for ISLs and future growth.
- At a minimum, two core switches and three edge switches are required to implement the core-edge fabric.

## IP SAN, FCoE and NVMe-oF

## IP SAN, FCoE and NVMe-oF

## Overview of IP SAN

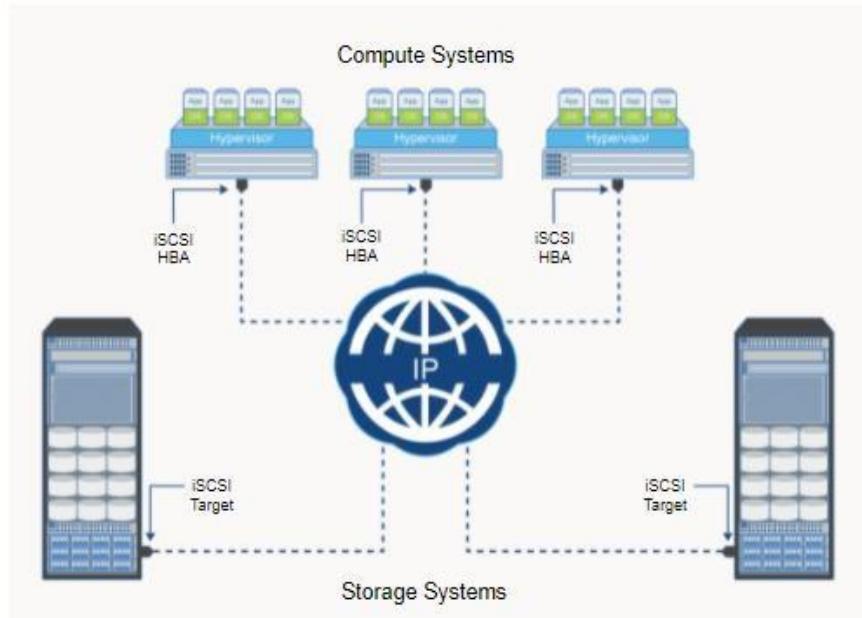
## Module Objectives

The main objectives of the module are to:

- Explain the advantages of implementing an IP SAN compared with an FC SAN.
- Define iSCSI components, and IP network connectivity.
- Explain the Fibre Channel over IP (FCIP) protocol, and how it is used to extend FC SANs over IP WAN.
- Define FCIP components, and FC SAN, and IP WAN connectivity.
- Explain Fibre Channel over Ethernet (FCoE).
- Explain NVMe Over Fabrics (NVMe-oF).

## Overview of IP SAN

## IP SAN Overview



*SCSI storage command paths over an IP SAN*

An IP SAN uses the Internet Protocol (IP) to transport storage block I/O data over a LAN.

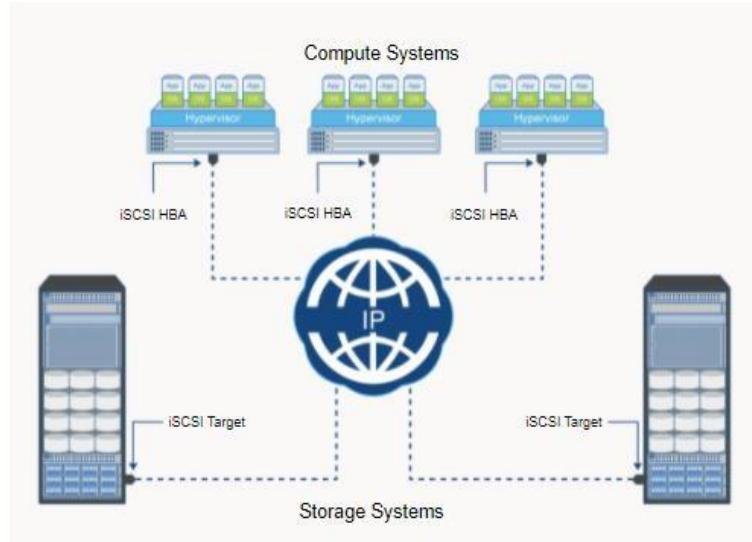
Users might choose to implement a SAN over IP because they want to use their existing IP network. This method is more cost effective than implementing a new Fibre Channel SAN.

- Operations and management personnel that already understand the LAN and IP network do not have to learn new Fibre Channel administration and management skills.
- Existing network security principles and protocols remain unchanged, and apply to storage data traffic layered over an IP network.
- The LAN must handle the continuous and peak demands of the storage traffic load without impacting normal user data traffic.
- Many organizations build smaller, separate LAN infrastructures to host IP SANs when the existing LAN cannot handle the full block storage traffic load. Where needed, separate IP SANs can be interconnected using standard network routers.

## IP SAN Protocols

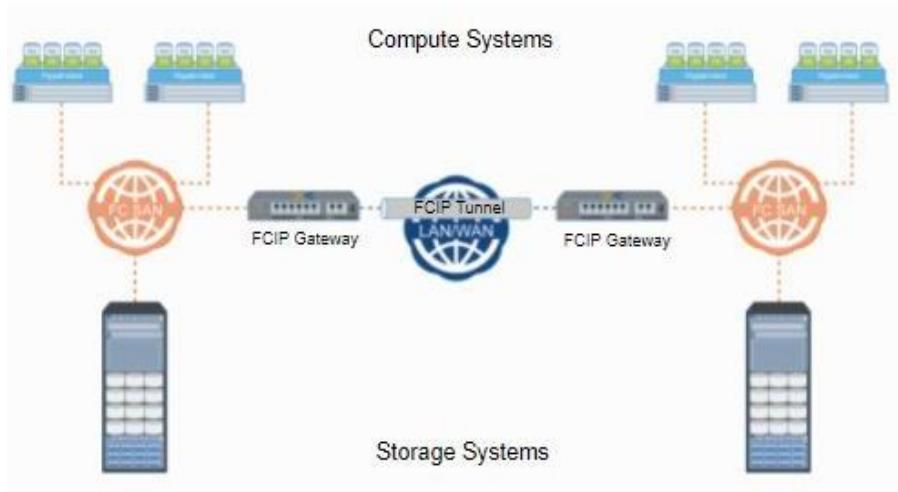
There are two storage data transport protocols that are hosted on an IP network.

### iSCSI



- IP-based protocol that enables transporting SCSI data over an IP network
- Encapsulates SCSI I/O into IP packets and transports them using TCP/IP.
- iSCSI is widely adopted for transferring SCSI storage data over IP between compute and storage systems, and among the storage systems.
- iSCSI is an inexpensive and easy way to implement a fully functional SAN.

## FCIP



- IP-based protocol that is used to interconnect distributed FC SAN islands over an IP network.
- Encapsulates FC frames onto IP packet and transports over existing IP network.
- Enables transmission by tunneling data between FC SAN islands.
- FCIP is used to interconnects FC SANs over an IP network. The protocol transports the Fibre Channel protocol and the SCSI block I/O data it carries over long distances, interconnecting geographically dispersed FC SANs.
- The best way to interconnect geographically dispersed FC SANs over WAN distances is through reliable, high-speed network links.

### Notes:

iSCSI and FCIP are used for different purposes due to inherent performance and reliability differences.

iSCSI is typically confined to a LAN infrastructure. Compute-to-storage SAN operations demand the reliable, low latency and rapid response times afforded by short distances between interconnected devices.

FCIP interconnects FC SANs over WAN distances. WANs are subject to unreliability, high latency and slow response times. Therefore, FCIP is typically limited to:

## Overview of IP SAN

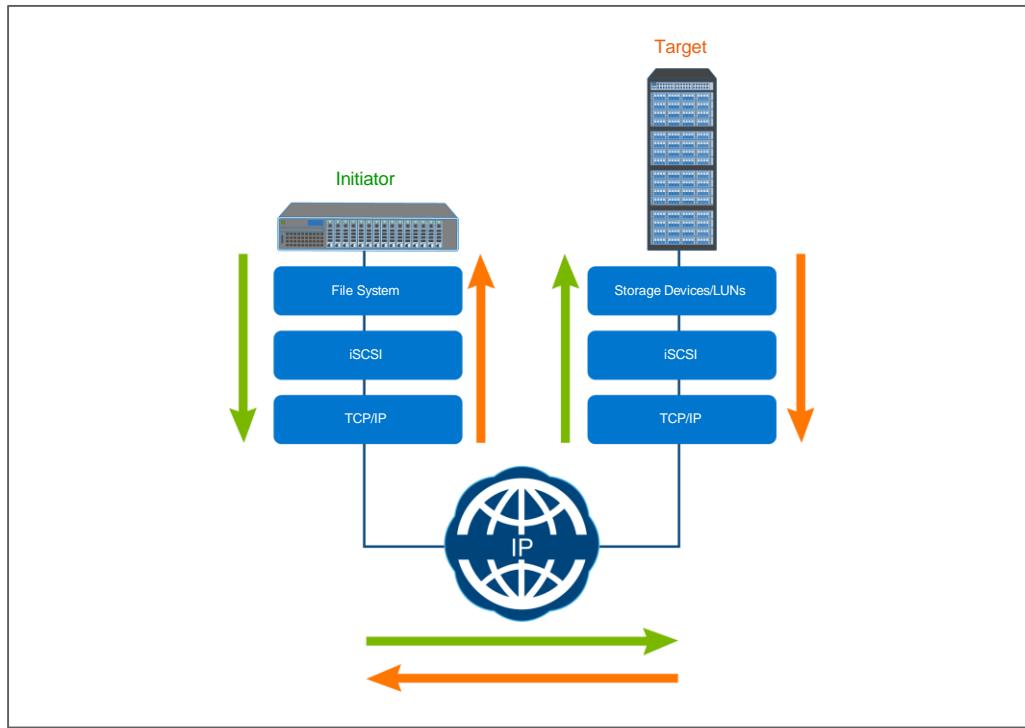
- Interconnecting production FC SANs with remote FC SANs used mainly to store non-production replication and backup data.
- Populating edge computing data center FC SANs with storage data from the main data center. FCIP can also be used to keep edge and main data center information in sync.

iSCSI

## iSCSI

## iSCSI Overview

SCSI commands and data are placed as payload into IP packets, and the TCP/IP protocol provides reliability, and flow control.

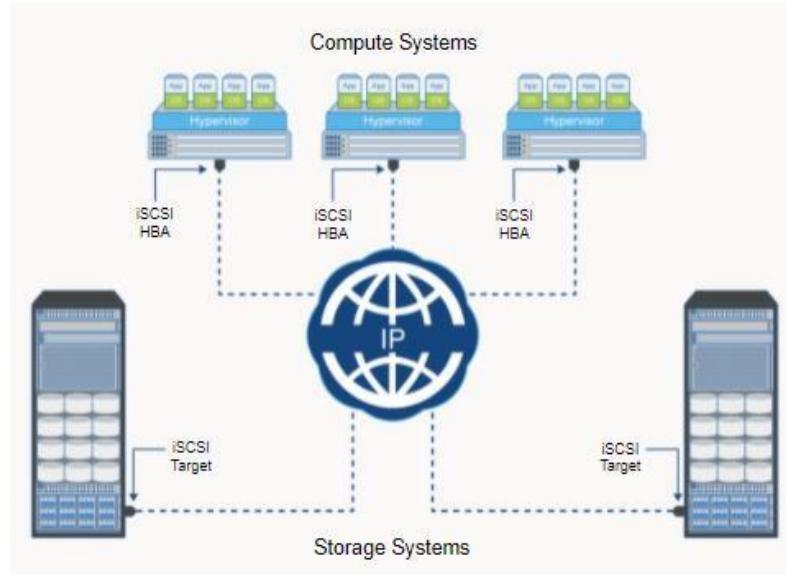


The SCSI protocol remains unchanged in how it functions, even when transported over Fibre Channel or IP networks.

- The SCSI storage I/O protocol uses the labels *Initiator* and *Target* to identify devices that connect and communicate with each other through the SCSI protocol.
- A source device, typically a compute node or host, contacts and requests a connection to the storage device that contains data it needs to read or update.
- The storage device that responds and establishes the connection is considered the target device.

## iSCSI Components

Key components for iSCSI communication are:



*iSCSI HBAs (Initiators) and iSCSI Target*

- iSCSI initiators
  - Example: iSCSI HBA
- iSCSI targets
  - Example: Storage system with iSCSI port
- IP-based network
  - Example: Gigabit Ethernet LAN

### Notes:

Software iSCSI initiator operations are performed by the server operating system. Software iSCSI consumes CPU processing power that should be reserved for the applications.

A hardware iSCSI initiator is a dedicated, host-based NIC designed to handle the iSCSI processing functions, removing the processing demand from the server's CPUs.

Following are the common examples of iSCSI initiators:

## iSCSI

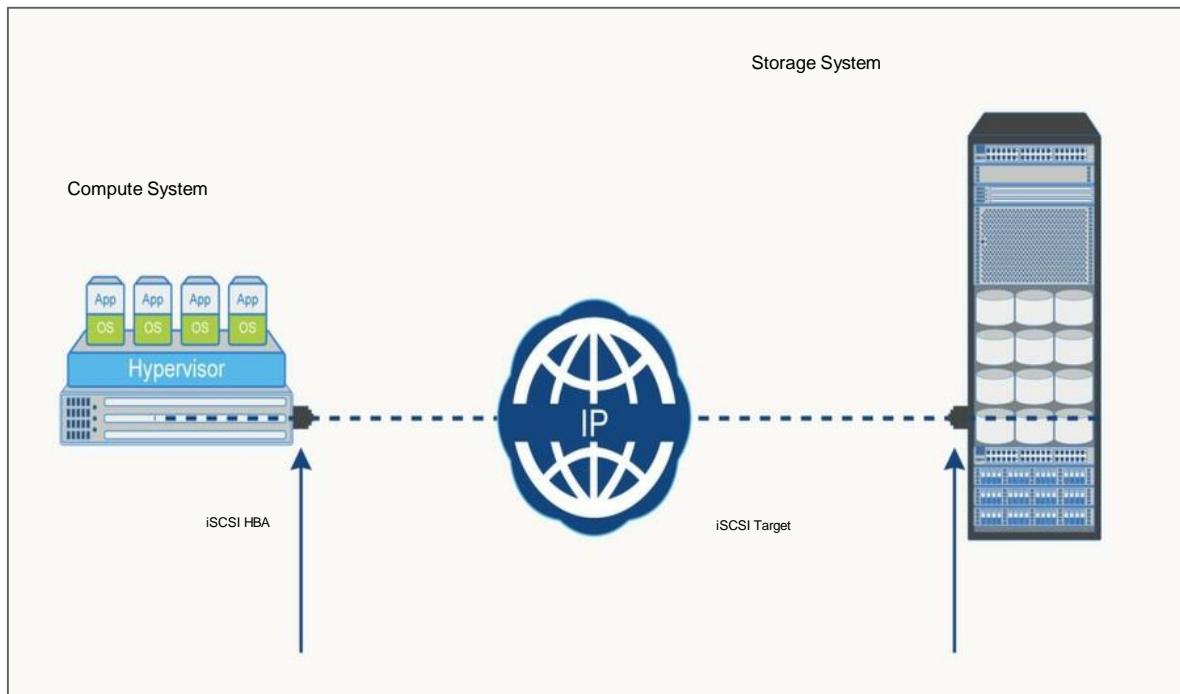
- **Standard NIC with software iSCSI adapter:** The iSCSI initiator is part of the operating system software. TCP/IP processing and the encapsulation of SCSI data into IP packets are carried out by the server CPU, so standard embedded or add-on Ethernet NICs can be used. It is least expensive and easy to implement. A software iSCSI initiator places higher demands on the server's CPUs. In heavy I/O load situations, the extra CPU load might slow application processing.
- **TOE NIC with software iSCSI adapter:** A TOE NIC offloads the TCP/IP processing from the server's CPUs, and leaves only the iSCSI functionality to be processed. The compute system passes the iSCSI information to the TOE NIC and then the TOE NIC sends the information to the target system through TCP/IP. Although this arrangement improves performance, the iSCSI functionality is still handled by a software adapter that requires server CPU processing.
- **iSCSI HBA:** An iSCSI HBA is a hardware adapter with built-in iSCSI functionality. It is capable of providing performance benefits over software iSCSI adapters by offloading the entire iSCSI and TCP/IP processing from the server's CPU's.

## Native and Bridged iSCSI Connectivity

iSCSI implementations support two types of connectivity: native and bridged.

***Click the tabs to understand the connectivity options.***

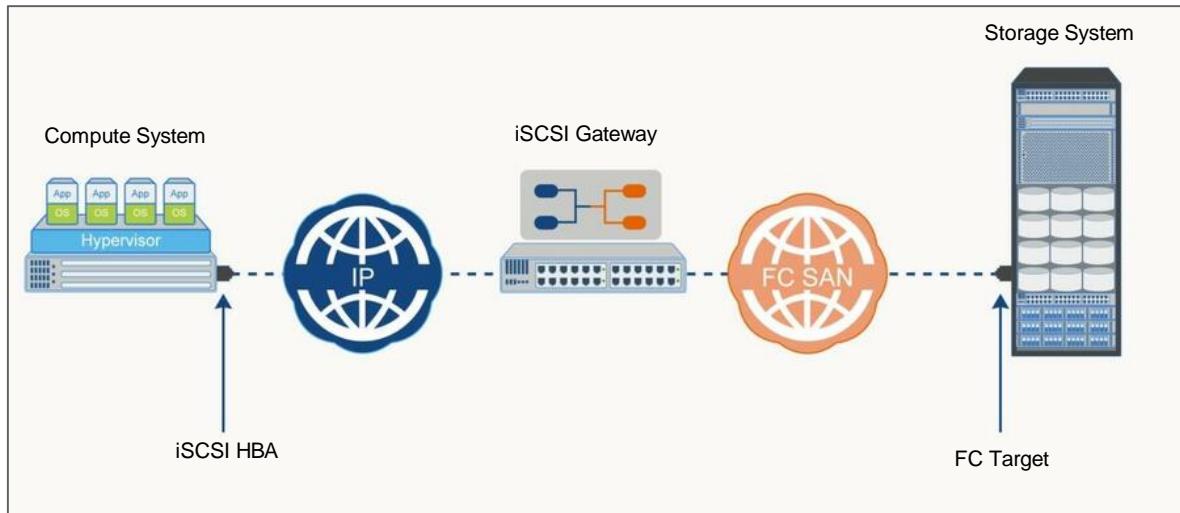
### Native



- iSCSI initiators connect to iSCSI targets directly through IP network.
- No Fibre Channel components.

## iSCSI

### Bridged



- iSCSI initiators are attached to IP network.
- Storage systems are attached to FC SAN.
- iSCSI gateway provides bridging functionality.

#### Notes:

**Native iSCSI:** In this type of connectivity, the compute systems with iSCSI initiators may be either directly attached to the iSCSI targets or connected through an IP-based network. FC components are not required for native iSCSI connectivity. The figure in the left tab shows a native iSCSI implementation that includes a storage system with an iSCSI port. The storage system is connected to an IP network. After an iSCSI initiator is logged on to the network, it can access the available LUNs on the storage system.

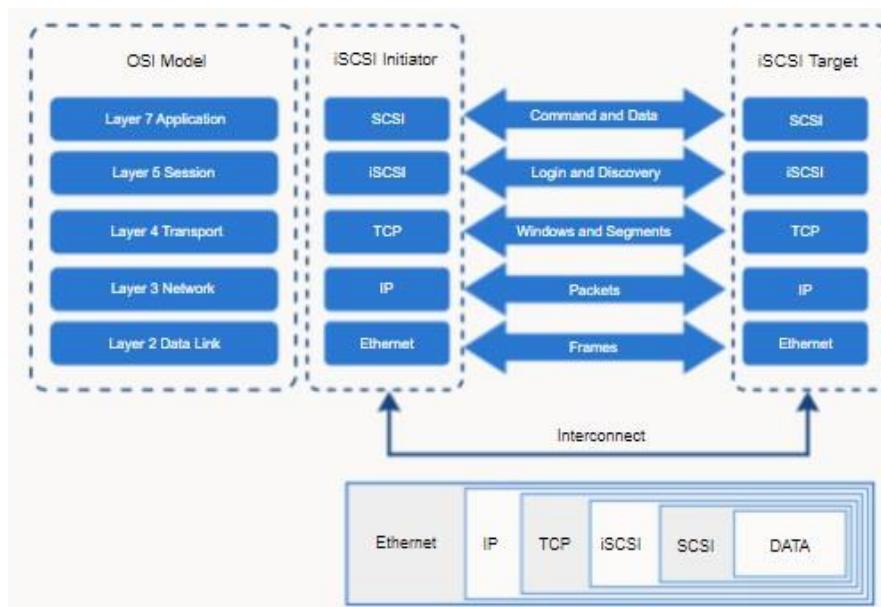
**Bridged iSCSI:** A Fibre Channel only storage system does not have Ethernet ports for iSCSI. In this case, a multiprotocol router or gateway is required. The gateway has both Fibre Channel and Ethernet iSCSI ports to serve as a proxy, allowing the FC storage system to participate in the iSCSI SAN. The gateway encapsulates FC frames into IP packets thus bridging the connectivity between the IP and FC environments. FC frames destined for the storage system are decapsulated from IP packets then forwarded to the native FC interfaces.

iSCSI initiators are configured with the gateway's IP address as the target destination. On the storage system facing side, the gateway is configured as an FC initiator.

iSCSI bridging is not required for storage systems that are equipped with both FC and Ethernet iSCSI ports.

## iSCSI Protocol Stack

The image displays a detailed model of how iSCSI protocol layers map into the OSI network model. It also shows the encapsulation order of iSCSI, and native SCSI commands and data for transport over the Ethernet LAN and IP network.



*iSCSI protocol stack and Ethernet encapsulation*

- SCSI commands, data, and status are encapsulated into TCP/IP and transported over the network.
- SCSI initiators and targets implement similar network stacks to establish and maintain communications.
- The iSCSI session-layer protocol initiates a reliable session between devices.
- TCP is used with iSCSI at the transport layer to provide reliable transmission.

### Notes:

iSCSI is the session-layer protocol that initiates a reliable session between devices that recognize SCSI commands and TCP/IP. The iSCSI session-layer interface is responsible for handling login, authentication, target discovery, and session management.

TCP is used with iSCSI at the transport layer to provide reliable transmission. TCP controls message flow, windowing, error recovery, and retransmission. It relies upon the network layer of the OSI model to provide global addressing and connectivity. The OSI Layer 2 protocols at the Data Link Layer of this model enable node-to-node communication through a physical network.

## iSCSI Addressing and Naming

### Common Types of iSCSI Name

- IQN: iSCSI Qualified Name

iqn.2008-02.com.example:optional\_string

- EUI: Extended Unique Identifier

eui.0300732A32598D26

- NAA: Network Address Authority

naa.52004567BA64678D

An iSCSI address is the logical path to an iSCSI initiator or target. It consists of:

- Location of iSCSI initiator or target.
  - Combination of IP address and TCP port number.
- iSCSI name
  - Unique identifier for initiator or target in an iSCSI network.

### Notes:

**iSCSI Address:** An iSCSI address indicates the location of an iSCSI initiator or target on the network, and the iSCSI name. The location is a combination of the host name or IP address and the TCP port number. For iSCSI initiators, the TCP port number is omitted from the address.

**iSCSI Name:** The iSCSI name is a unique worldwide iSCSI name that is used to identify initiators and targets within an iSCSI network. The unique identifier can be a combination of the names of the department, application, manufacturer, serial

number, asset number, or any tag that can be used to recognize and manage the iSCSI nodes.

The following are three types of iSCSI names commonly used:

- **iSCSI Qualified Name (IQN):** An organization must own a registered domain name to generate iSCSI Qualified Names. This domain name does not need to be active or resolve to an address. It needs to be reserved to prevent other organizations from using the same domain name to generate iSCSI names. A date is included in the name to avoid potential conflicts caused by the transfer of domain names.

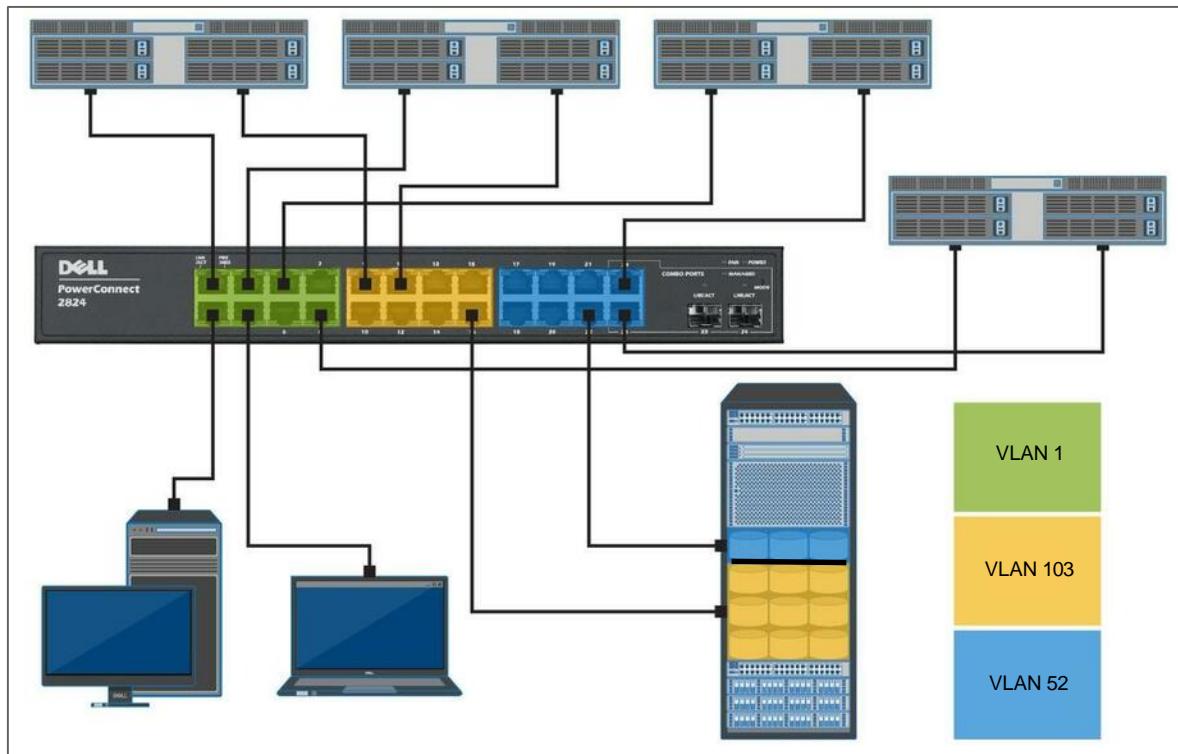
An example of an IQN is *iqn.2015-04.com.example:optional\_string*.

The optional string provides a serial number, an asset number, or any other device identifiers. IQN enables storage administrators to assign meaningful names to the iSCSI initiators and the iSCSI targets, and therefore, manages those devices more easily.

- **Extended Unique Identifier (EUI):** An EUI is a globally unique identifier based on the IEEE EUI-64 naming standard. An EUI is composed of the eui prefix followed by a 16-character hexadecimal name, such as eui.0300732A32598D26.
- **Network Address Authority (NAA):** NAA is another worldwide unique naming format as defined by the International Committee for Information Technology Standards (INCITS) T10 – Fibre Channel (FC) protocols committee. This format enables SCSI storage devices that contain iSCSI ports and other ports types, such as SAS and FC, to use the same NAA-based SCSI device name.

An NAA is composed of the naa prefix followed by a hexadecimal name, such as naa.52004567BA64678D. The hexadecimal representation has a maximum size of 32 characters (128 bit identifier).

## Virtual LAN (VLAN)



A VLAN is one or more *logical* Ethernet LANs that operate over a single physical Ethernet LAN infrastructure. VLANs are used to isolate communications between a group of nodes, independent of their location across the physical network. A VLAN has the following characteristics:

- Fully independent functionality. Each VLAN operates exactly as a physical LAN, but with its own set of protocols and services.
- The physical LAN is used to provide hardware level connectivity, and maintain transport paths to carry its hosted VLANs.
- A VLAN operates, and is managed as a single administrative network domain.
- VLANs are well suited for iSCSI deployments as they enable full iSCSI traffic isolation from other, non-SAN network traffic. Using VLANs for iSCSI provides high security due to full operational isolation between each IP SAN.

### Notes:

Configuring a VLAN over a physical LAN network includes:

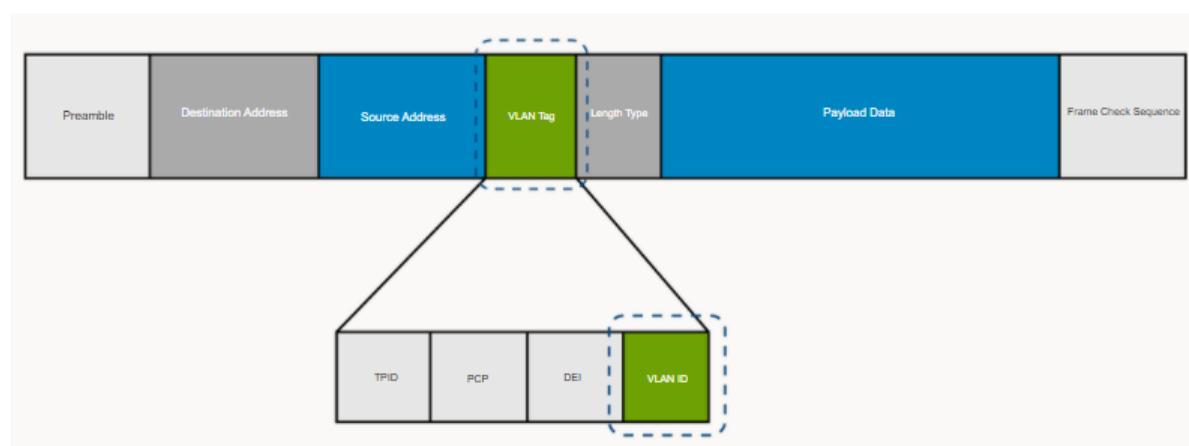
- Defining VLANs over the physical LAN. Each VLAN is identified with a unique VLAN ID.
- Configuring VLAN membership. VLANs can be configured at different layers of the protocol stack in the network. The example maps VLAN membership to OSI model layer definitions.
  - **Physical Layer 1** - Membership based on assigning a switch port to the VLAN. Any host attached to a port must become a member of the port assigned VLAN.
  - **Data Link Layer 2** - Membership based on the unique Ethernet MAC address of a host NIC port or protocol type. This method allows a host to be moved to other physical switch ports but remain in the same VLAN.
  - **Network Layer 3** - Membership is based on the network address portion of the IP address. For example: 192.168.20 = VLAN 2, 192.168.30 = VLAN 3. This method allows hosts to be relocated without reconfiguring their IP address. Network layer VLAN assignment does not involve nor change network routing configurations.
  - **Application Layer 7** - Membership is based on a particular application such as File Transport Protocol (FTP) or Telnet. An example is where FTP is transported only across VLAN 40 and Telnet across only VLAN 45.

## VLAN Tagging

VLAN tagging is performed by inserting a 4-byte tag field containing a 12-bit VLAN ID into the Ethernet frame before it is transmitted through an interswitch trunk link. The receiving switch reads the tag and forwards the frame to the destination ports that corresponds to that VLAN ID. The tag is removed once the frame leaves a trunk link to reach a node port.

### Ethernet Frame with VLAN Tag Format

Ethernet switches that have VLAN enabled use Ethernet frames with the VLAN TAG field added. The VLAN TAG is a 12-bit field that can address up to 4096 VLANs. A switch reads the VLAN tag and forwards the Ethernet frame to the port assigned to the VLAN ID, or to the next switch when required.



*The diagram shows an Ethernet frame with an IEEE 802.1Q VLAN tag inserted. VLAN enabled switches use this format to forward Ethernet frames between switches and ports according to the VLAN Tag*



Large cloud environments may require more than the maximum 4096 VLANs. The IEEE 802.1ad standard provides for using two VLAN TAG fields in an Ethernet frame. Two VLAN TAG fields increase the number of addressable VLANs to 16,777,216.

## iSCSI: Additional Information



To understand about iSCSI protocol, click [here](#).

Knowledge Check

## Knowledge Check

## Knowledge Check

1. Which type of iSCSI NIC offloads both iSCSI and TCP/IP protocol processing from the host?
  - a. iSCSI HBA
  - b. TOE card
  - c. Standard NIC with software iSCSI adapter
  - d. Gigabit Ethernet NIC with software iSCSI adapter

## Knowledge Check

### Knowledge Check

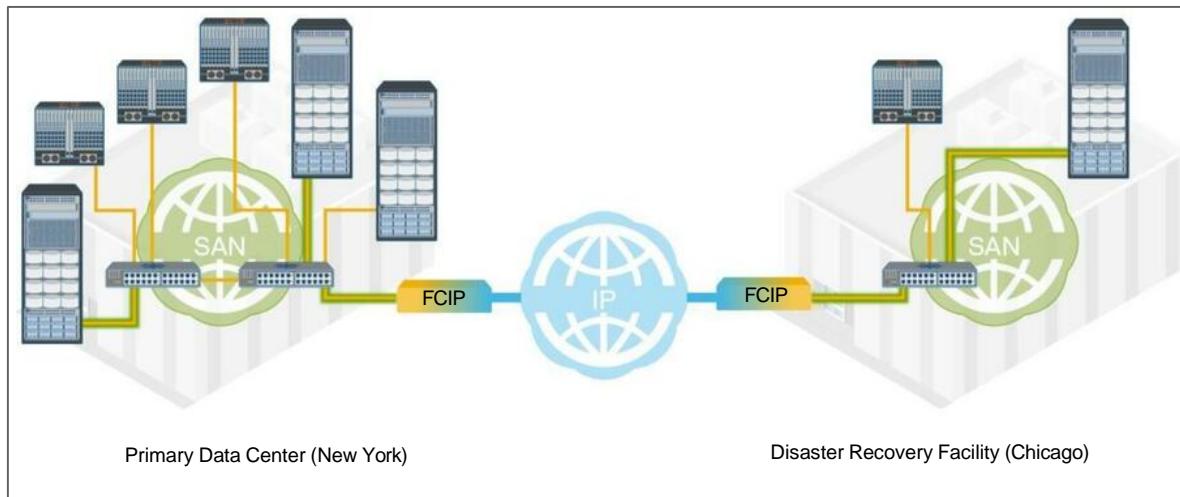
2. Match each VLAN membership type with its OSI protocol stack implementation layer.

A. Membership is based on assigning a switch port to the VLAN.	<u>A</u>	Physical Layer 1
B. Membership is based on the network address portion of the IP address.	<u>D</u>	Data Link Layer 2
C. Membership is based on a particular application such as File Transport Protocol (FTP) or Telnet.	<u>B</u>	Network Layer 3
D. Membership based on the unique Ethernet MAC address of a host NIC port.	<u>C</u>	Application Layer 7

# FCIP

## FCIP Overview

## Fibre Channel Over IP (FCIP)



*FCIP Connectivity for remote FC SAN device*

FCIP is a tunneling protocol that encapsulates Fibre Channel frames into IP packets. FCIP uses an IP network to transport FC SAN traffic. The purpose of FCIP is to extend an FC SAN over distances that exceeds the maximum native Fibre Channel connectivity of about 200 km (125 miles). The primary use of FCIP is to interconnect FC storage systems over WAN distances.

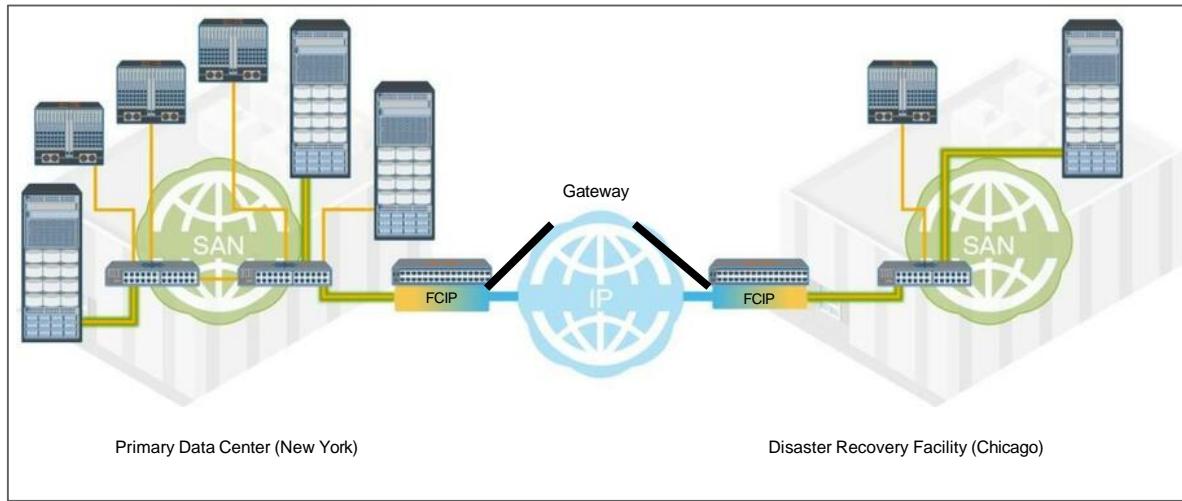
- Organizations use FCIP to interconnect their main FC SAN to geographically remote FC SANs for business continuity and disaster recovery.
- FCIP interconnects local and remote FC SANs so that local production block storage data can be seamlessly copied to remote sites.
  - Copying data can be continuous, using replication techniques or scheduled periodically during daily backup windows.
  - Replication is preferred over periodic data backup applications typically not sensitive to IP WAN low bandwidth and high latency.
- FCIP uses TCP for flow control and in-order packet delivery.
  - Using TCP also ensures in-order FC frame delivery, which is required for normal operation of FC SANs.

## FCIP Connectivity

FCIP implantation does not require modifying an FC SAN. A special multiprotocol switch, also known as an *FCIP gateway* is connected to each FC SAN. The multiprotocol switch contains both FC and Ethernet ports. At each FC SAN, the FC port is configured as an E\_Port and is connected to an FC switch. This port receives FC frames and sends them to be encapsulated into IP packets that are forwarded to the Ethernet port. The Ethernet port is connected to the LAN, and routed to the WAN that connects to the remote facility.

At the remote facility, the incoming WAN connection is routed to the receiving multiprotocol switch LAN port.

The FC frame payload data is decapsulated and forwarded to the FC port that is also configured as an E\_Port. FC frames are transported to the native FC SAN switch and forwarded to the destination storage system.



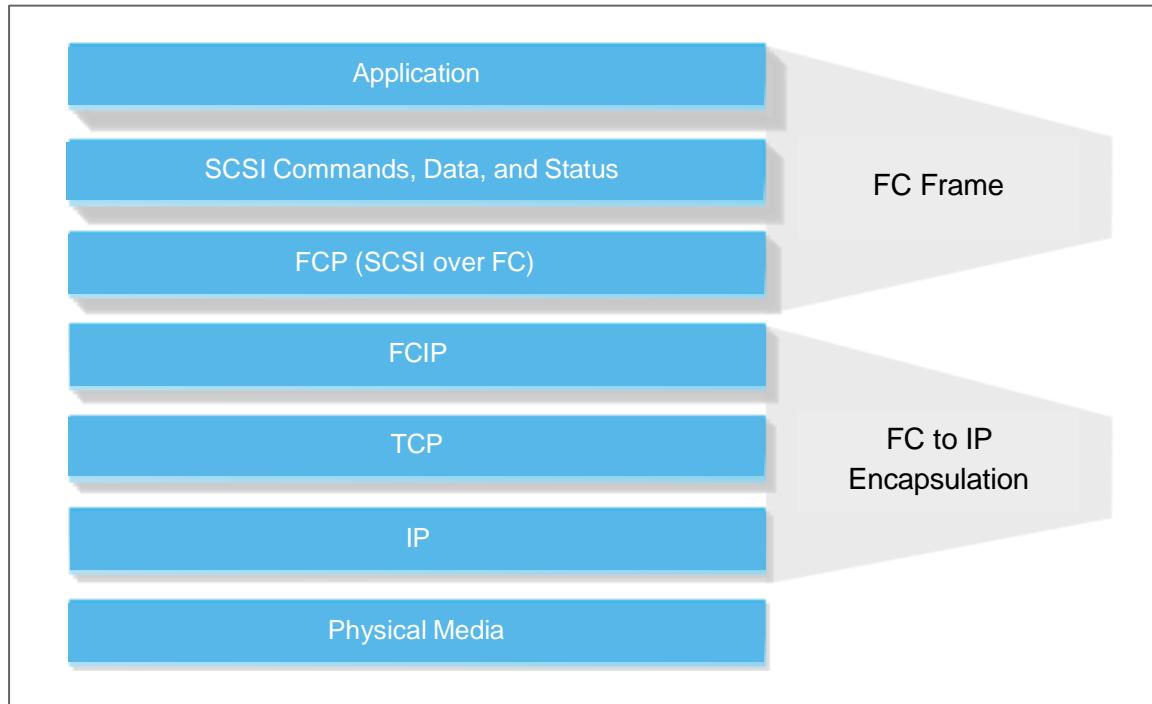
*The image shows FCIP gateways with FC SAN facing E\_Ports, and network facing NIC ports. These ports connect the source and remote FC SANs over the IP WAN.*

## FCIP Protocol Stack and Frame Encapsulation

### Protocol Stack

The FCIP protocol stack is shown on the image.

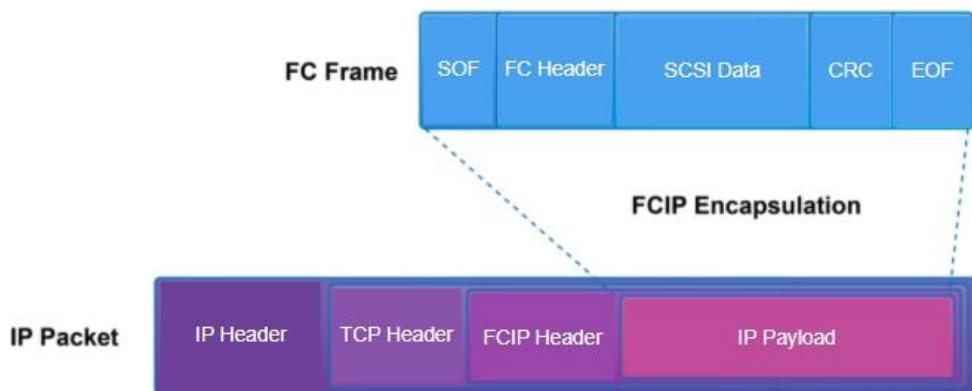
- Applications generate SCSI commands and data, which are processed by various layers of the protocol stack.
- The upper layer protocol SCSI includes the SCSI driver program that runs the read-and-write commands.
- Below the SCSI layer is the FC protocol (FCP) layer, which is an FC frame whose payload is the SCSI protocol.
- The FC frames can be encapsulated into the IP packet and sent to a remote FC SAN over the IP.
- The FCIP layer encapsulates the FC frames onto the IP payload and passes them to the TCP layer.
- TCP and IP are used for transporting the encapsulated information across Ethernet, wireless, or other media that support the TCP/IP traffic.



### Encapsulation

Encapsulation of an FC frame onto an IP packet could cause the IP packet to be fragmented. The fragmentation occurs when the data link cannot support the maximum transmission unit (MTU) size of an IP packet.

- The required parts of the header must be copied by all fragments an IP packet is fragmented.
- TCP operations are responsible for receiving and resequencing the data when a TCP packet is segmented.
- The receiving and resequencing is performed before passing it on to the FC processing portion of the device.



## FCIP Connectivity: Additional Information



*To understand about FCIP connectivity, click [here](#).*

## Knowledge Check

## Knowledge Check

### Knowledge Check

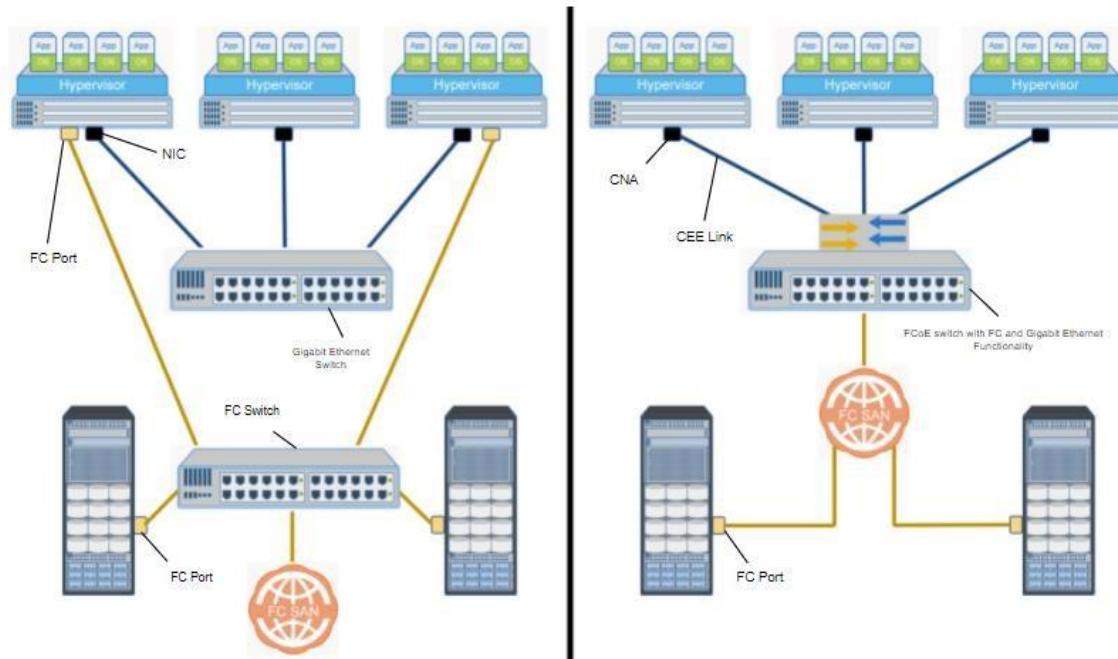
1. What type of network switch is used to connect FC SANs over an IP WAN?
  - a. Multiprotocol switch
  - b. Managed switch
  - c. Unmanaged switch
  - d. PoE switch

FCoE

FCoE

## FCoE Overview

## Fibre Channel Over Ethernet (FCoE)



FCoE is a storage protocol that enables Fibre channel SAN traffic to run directly over an existing 10 Gigabit or greater Ethernet LAN infrastructure. FCoE converges Fibre Channel and Ethernet protocols over a single interface adapter and cable. FCoE is used to converge these two types of networks to:

- Consolidate networking connectivity points.
- Reduce physical FC and Ethernet switch infrastructure complexity.
- Reduce the number of cables, NIC cards, and ports.
- Eliminate the expense of implementing and administering an FC SAN infrastructure.

**Diagram on the left:** Separate FC SAN and Ethernet LAN. All systems communicate through the LAN, with two of the host systems accessing both the LAN and their storage data over the separate FC SAN.

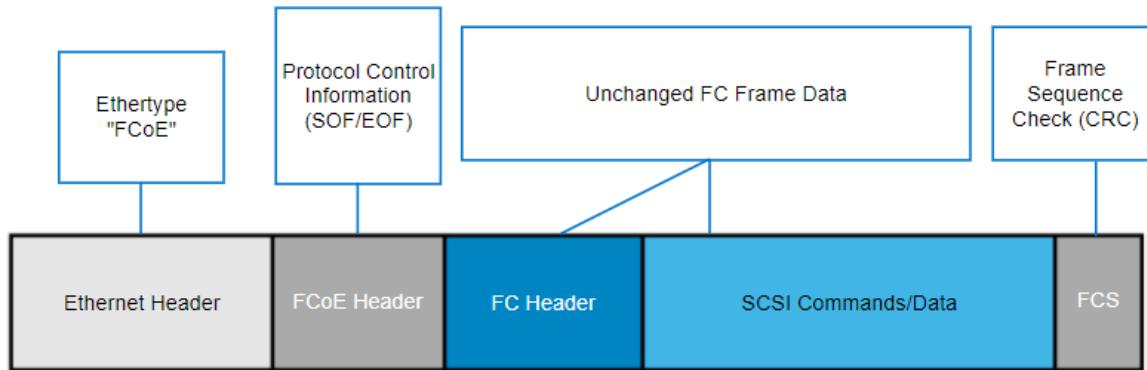
**Diagram on the right:** Converged FC SAN and Ethernet network using special FCoE switches. FCoE switches each have Gigabit Ethernet and Fibre Channel ports. A special converged network adapter (CNA) is installed in each host system that requires both LAN and FC SAN connectivity. The CNA replaces the NIC and FC HBA adapters. It connects to both FC SAN and Ethernet LAN

## FCoE

through a single port that is connected to an FCoE switch. Converged LAN and SAN traffic is separated before being forwarded to the host operating system and applications.

## FC Frame Encapsulation

FCoE encapsulates unchanged FC frames into Ethernet frames as the payload. Below is an example of FCoE frame encapsulation.



*The image shows an FCoE Ethernet frame carrying an unchanged Fibre Channel frame as its payload*



**Tip:** Since Fibre Channel is a lossless protocol, the converged Ethernet network must also conform to the Data Center Bridging (DCB)<sup>54</sup> standards.

<sup>54</sup> Fibre Channel requires a consistent, lossless transport to operate correctly. FCoE uses the Data Center Bridging (DCB) standards to achieve this requirement. DCB is a set of enhancements applied to an Ethernet LAN when it is used for converged networking. DCB reduces or eliminates data frame loss that occurs during times of even minimal network congestion. It uses priority-based flow control to reduce or eliminate network frame and packet loss. DCB does not use TCP because flow control is performed at the Ethernet Data Link layer.

## FCoE: Additional Information

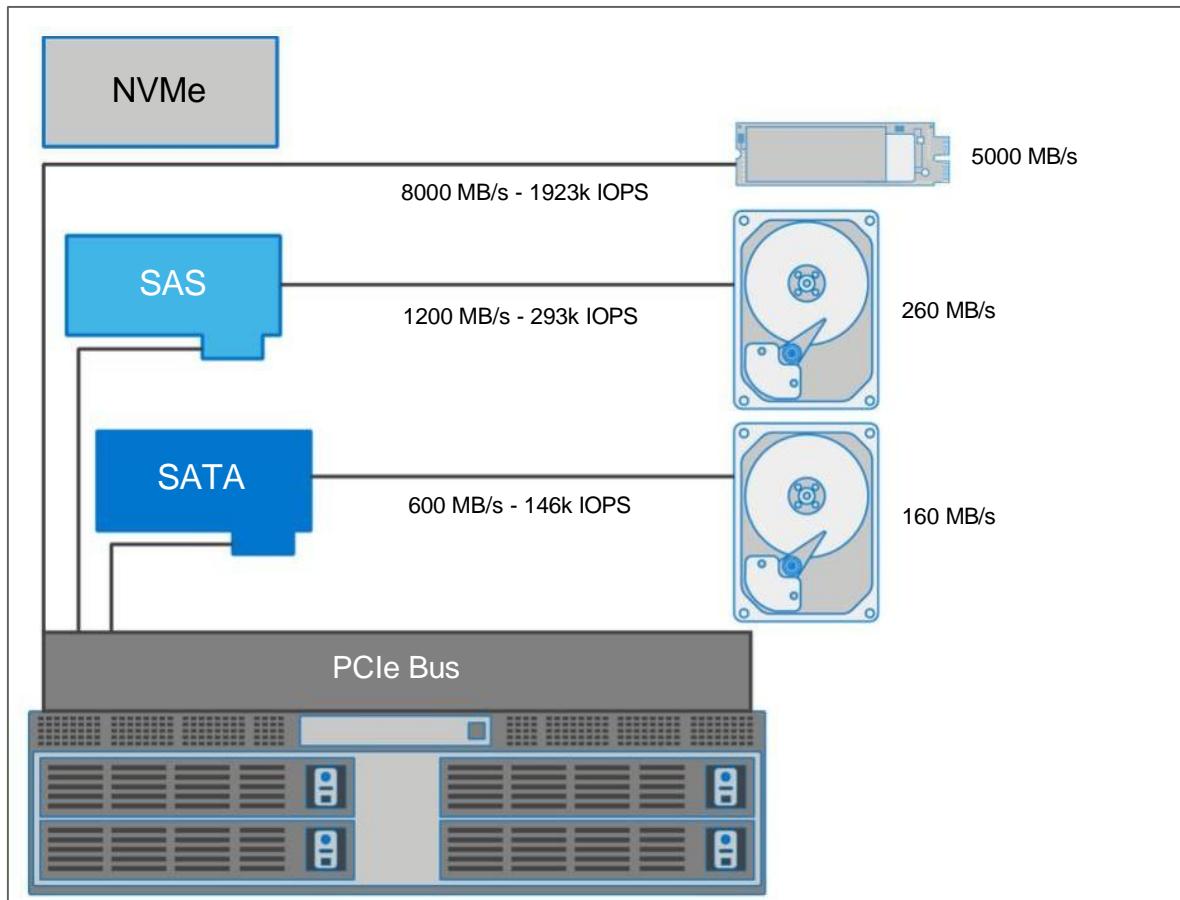


*To understand about FCoE connectivity, click [here](#).*

## NVMe Over Fabrics

## NVMe Over Fabrics Overview

## NVM Express Overview



*The image matches SATA, SAS, and NVMe interface performance with maximum attached storage device capabilities*

NVM is used in Solid-State disks (SSD) and M.2 format storage devices that replace the spinning disk drives in hosts and storage systems. An NVM device is faster than spinning disk, and provides low data transfer latency.

- NVM Express (NVMe) is a computer-to-disk connectivity protocol that is developed for use with Non-Volatile Memory (NVM) storage devices.
- An NVMe device connects directly to an embedded storage controller on the motherboard instead of a PCIe card. The embedded controller allows the NVMe device to achieve maximum performance.

Beyond higher data transfer speeds and low latency, NVMe offers these SCSI command operation enhancements:

## NVMe Over Fabrics

- Up to 64,000 SCSI command queues to improve SCSI command processing and completion.
- Each NVMe SCSI command queue can store up to 64,000 SCSI commands for rapid dispatch.
- Smaller CPU command set increases storage protocol stack I/O processing efficiency for higher throughput (IOPS).

### **Notes:**

Commonly known as *flash storage*, NVM devices are faster than spinning disk, and provides for low data transfer latency. Standard computer-to-disk connectivity protocols such as SCSI, SATA, and SAS are too slow to take advantage of the extreme performance available with NVM devices.

NVM Express (NVMe) is a computer-to-disk connectivity protocol that was developed for use with NVM storage devices.

An NVMe device connects directly to an embedded storage controller on the motherboard instead of a PCIe card. Because it is physically closer to the CPUs, the embedded controller allows the NVM device to achieve maximum performance.

## NVMe Over Fabrics

Native NVMe cannot connect to NVM storage devices outside of the server. NVMe Over Fabrics (NVMe-oF) was introduced to enable shared NVMe storage device connectivity. NVMe Over Fabrics enables the NVMe protocol to be transported over FC or other fabrics. NVMe-oF enables servers to take full advantage of high performance NVM flash storage systems distributed across a SAN fabric.

### Drivers for NVMe Over Fabrics

Data center virtualization, applications, and converged infrastructure servers with high storage I/O and capacity requirements is growing. These demands cannot be met with native NVMe because it cannot scale beyond the server. Other networked storage sharing architectures may be used to share NVMe devices, but they limit the performance capabilities of NVMe devices.

- **Server-based SAN:** Solutions such as Dell EMC PowerFlex or VMware VSAN allow servers to share NVMe and other internal storage capacity with each other. However, the high-speed NVMe protocol is still limited to operate internally at the server.
- **Standard FC SAN:** FC SANs deliver high shared storage performance through Fibre Channel and networked All-Flash, NVM storage systems. However, standard FC-SAN environments with standard All-Flash storage systems cannot use the NVMe protocol to take full advantage of NVMe device performance.
- **32 Gb/s FC SAN with NVMe-oF:** NVMe-oF takes advantage of the end-to-end I/O operation enhancements of SAN fabrics. These SAN fabrics can be based on 32 Gb/s Fibre Channel, and 10 Gigabit or greater Ethernet LANs with TCP.

### Notes:

Native NVMe cannot connect to NVM storage devices outside of the server. The only way to scale storage capacity and performance is to increase the number of physical servers with NVM devices. Servers that are already connected to a SAN are limited to using the higher latency FC-4 (SCSI) protocol to access the shared storage. Even if a high-performance NVM flash-based storage system is on the SAN, the servers could not take advantage of its increased capabilities.

## NVMe Over Fabrics

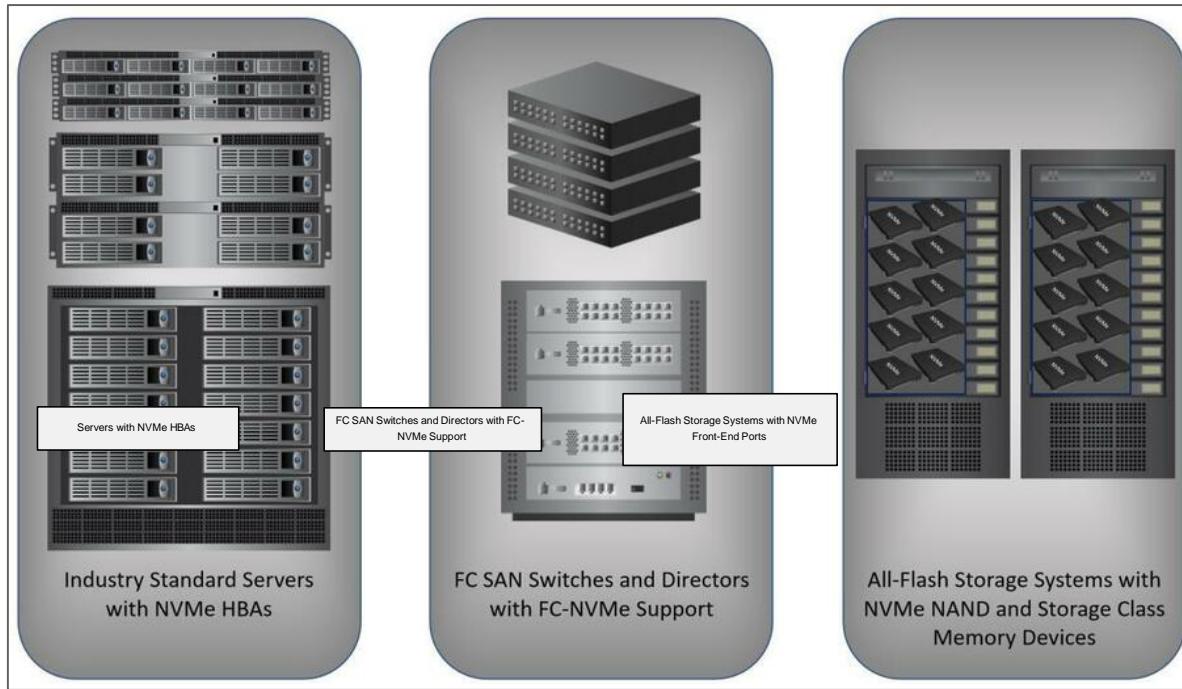
The number of data center virtualization, application, and converged infrastructure servers with high storage I/O and capacity demands is growing. These demands cannot be met with native NVMe because it cannot scale beyond the server.

Server-based SAN software such as Dell EMC PowerFlex or VMware VSAN allow servers to share internal NVMe and other internal storage with each other. However, server-based SANs have scaling and other limitations. The highest demanding environments require purpose-built, optimized networked storage systems such as All-Flash PowerMax. Also, data centers typically need multiple storage systems to provide high storage capacity, and distribute storage I/O load to rapidly scale with demand.

The advantage of NVMe-oF is that it adds scalable performance and capacity to the NVM storage benefits of higher speed and lower latency. NVMe-oF takes advantage of end-to-end I/O operation enhancements of SAN fabrics based on 32 Gb/s Fibre Channel, and 10 Gigabit or greater Ethernet LANs using TCP.

## NVMe Over Fibre Channel (FC-NVMe)

NVMe Over Fabrics relies on key technical features of the underlying storage network to efficiently transport the NVMe protocol. 32 Gb/s Fibre Channel fabrics provide:



*NVMe HBAs, FC-NVMe switches, and NVM storage systems are required to implement a fully functional FC-NVMe FC SAN (Click image to enlarge).*

- Reliable flow control and delivery.
- Consistently high speed and low end-to-end latency throughout the switched fabric.
- Transporting native NVMe commands directly through the fabric without requiring the FC-4 SCSI protocol layer.

Adding FC-NVMe to a standard FC SAN does not require modification to its general operation, management, and administration. However, FC-NVMe implementation requires specific server, SAN switch, and storage system features.

The diagram shows an FC SAN that is fully FC-NVMe enabled.

## NVMe Over Fabrics

Storage arrays with NAND<sup>55</sup> and Storage Class Memory (SCM)<sup>56</sup> devices are optimized to provide the highest FC-NVMe I/O performance and capacities.

---

<sup>55</sup> NAND is a type of nonvolatile flash memory. Nonvolatile memory does not require continuous power to retain stored data. Devices such as digital cameras, USB flash drives, smartphones, and SSD storage devices use NAND flash memory to store data.

<sup>56</sup> Storage class memory is a type of NAND flash storage device. This device includes a power backup to ensure that data will not be lost if power is removed. Power backup is required because SCM uses standard DIMM memory as a cache in front of the persistent NAND devices to greatly enhance performance. SCM devices are much faster, but more expensive than standard NAND devices such as SSDs. Storage class memory devices are used with, or replace slower persistent storage components such as SSDs.

## NVMe Over Fabrics Device Addressing

Similar to the iSCSI Qualified Name (IQN), NVMe -oF uses the NVMe Qualified Name (NQN) convention to identify a target on a networked NVMe storage system. The chart compares iSCSI and NVMe qualified name addressing conventions.

Protocol	Qualified Name Type	Address Example
iSCSI	IQN	iqn.1991-04.com.microsoft:kmrtd-srvr-d
NVMe Over Fabrics	NQN	nqn.2020-08.com.vendor:nvme:nvm-subsystem-sn-d48932

Knowledge Check

## Knowledge Check

## Knowledge Check

1. Which Qualified Name address format is used for NVMe-oF targets?
  - a. nqn.2020-08.com.vendor:nvme:nvm-subsystem-sn-d48932
  - b. eui.0300732A32598D26
  - c. naa.52004567BA64678D
  - d. iqn.1991-04.com.microsoft:kmrtd-srvr-d

## Concepts in Practice

## Concepts in Practice

### Dell EMC PowerSwitch S4100-ON

S4100 series switches provide switched LAN network connectivity for IP SANs.

- High-performance open networking top-of-rack switches with multirate Gigabit Ethernet and unified ports.
- The S4100-ON 10 GbE switches consist of Dell Technologies latest disaggregated hardware and software data center networking solutions. They provide state-of-the-art 100 GbE uplinks, Fibre Channel connectivity, and a broad range of functionality to meet the growing demands of the data center environment.
- These top-of-rack open networking switches offer optimum flexibility, and cost-effectiveness for the enterprise, midmarket and tier 2 cloud service providers.
- The S4100-ON series are high-performance, multifunction, 1/10/25/40/50/100 GbE and 8/16/32G FC top-of-rack (ToR) switches purpose-built for applications in high-performance data center, cloud, and computing environments.



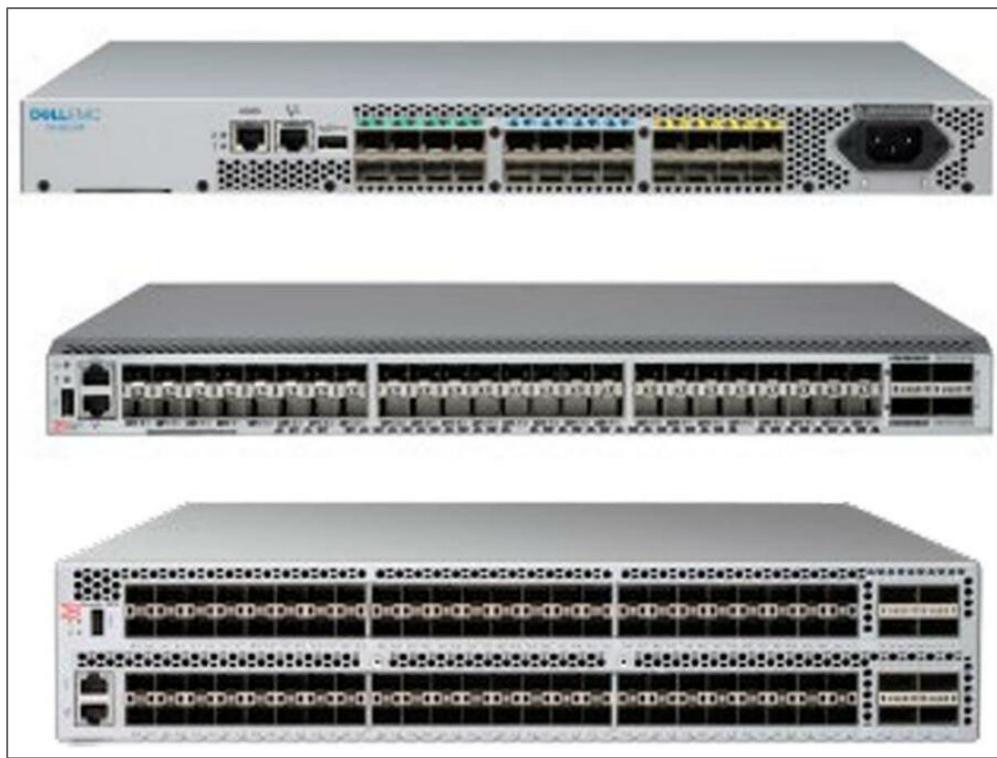
### Dell EMC Connectrix B-Series Switches

These Connectrix switches bring native NVMe-oF connectivity to an FC SAN. NVMe-oF is supported in 32 Gb/s models only.

- **DS-6600B** - Designed to support the SAN requirements of small-to-medium-sized environments, the Connectrix DS6610B is a 24-port switch that offers high performance and economy. The 1U base chassis is prepopulated with eight 6 Gb/s or 32 Gb/s Fibre Channel Small Form Factor Pluggable (SFP+) shortwave optics.

## Concepts in Practice

- **DS-6620B** - Designed to support the SAN requirements of medium-to large sized workgroups and that of large enterprises, the Connectrix DS-6620B offers forty-eight SFP+ ports and four QSFP ports in a 1U form factor. Two base models are available which have 24 active 32 Gb/s or 16 Gb/s ports, which are populated with 32 Gb or 16 Gb/s shortwave SFPs.
- **DS-6630B** - This model has 128 ports. There are 96 standard SFP 32 Gb/s capable ports and eight Quad Small Form-factor Pluggable (QSFP) ports which support an additional 32 ports.

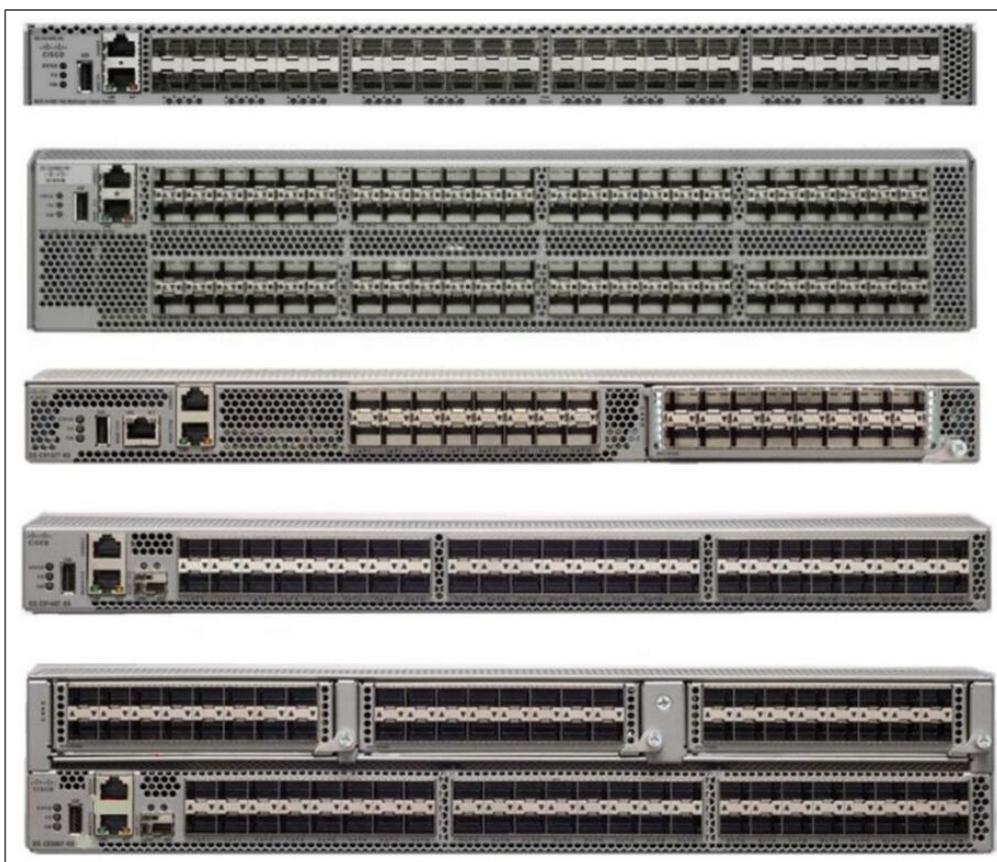


## Dell EMC Connectrix MDS Series Switches

The Connectrix MDS series contains two models in the Model S Fibre Channel Switch series, and three models in the Model T Fibre Channel Switch series. These MDS-series switches bring native NVMe-oF connectivity to an FC SAN. NVMe-oF is supported in all models.

- **MDS-9148S** - This 1 rack-unit switch scales from 12 to 48 line-rate 16 Gb/s Fibre Channel providing high performance with exceptional flexibility at effective cost. The MDS-9148S delivers speeds of 2, 4, 8 Gb/s and 16 Gb/s, with 16 Gb/s of dedicated bandwidth for each port.

- **MDS-9396S** - This 2 rack-unit (2RU) switch scales from 48 to 96 line-rate 16 Gb/s Fibre Channel ports. This switch scales to 96 ports.
- **MDS-9132T** - This 1 rack-unit switch scales from 8 to 32-port line-rate 32 Gb/s Fibre Channel ports. This switch provides high-speed Fibre Channel connectivity from the server rack to the SAN core directors.
- **MDS9148T** - This 1 rack-unit switch scales in 24, 32, 40 and 48-port increments. Medium and large-scale SAN architectures that are built with SAN core directors can expand 32 Gb/s connectivity to the server rack using these switches.
- **MDS-9396T** - This 2 rack-unit (2RU) switch scales in 48, 64, 80 and 96-port increments from 48 to 96 line-rate 32 Gb/s Fibre Channel ports. This switch provides high-speed connectivity in the SAN with high performance, density, and scale.

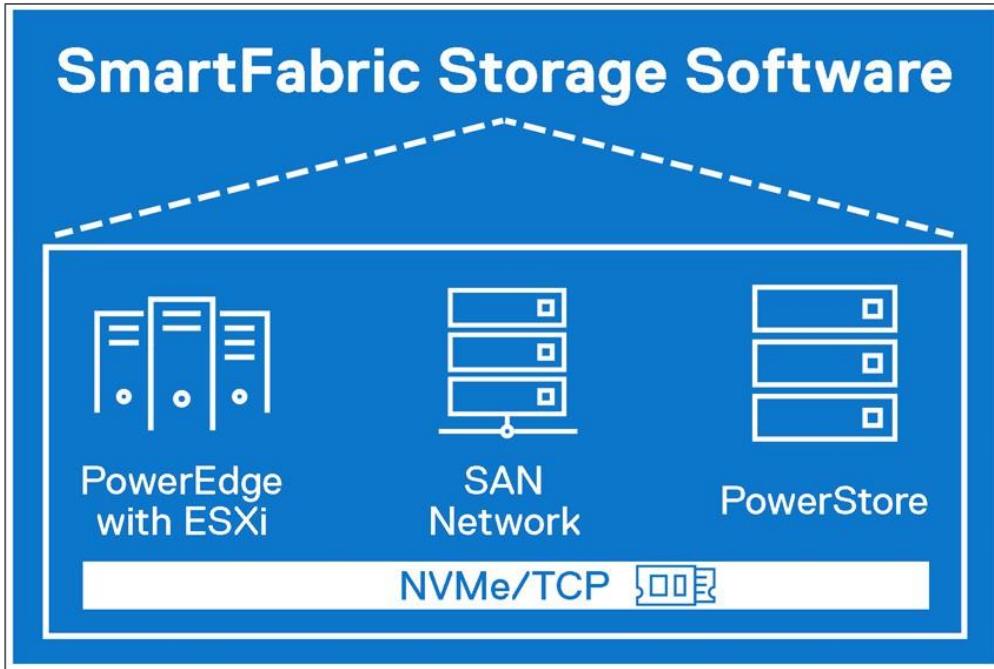


## SmartFabric Storage Software

In partnership with VMware, Dell Technologies has engineered a complete end-to-end NVMe/TCP solution to help provide enterprise organizations with the agility to stay ahead of growing workload demands with modern, automated, and secure storage connectivity both today and as they migrate to extended hybrid clouds.

The initial release of this solution consists of three main components:

- **SmartFabric Storage Software:** The Dell Technologies SmartFabric Storage Software (SFSS) product is a standards-based centralized discovery controller for NVMe/TCP servers and storage systems.
  - In its initial release, SFSS is a stand-alone containerized software solution. It enables an end-to-end automated and integrated NVMe-oF solution using TCP over an Ethernet fabric.
  - Main SFSS functions are policy-driven to help automate NVMe-oF storage service discovery, end-point registration, connectivity, and zoning.
- **PowerEdge with VMware ESXi and NVMe/TCP:** Deployed on PowerEdge servers running VMware ESXi. Takes advantage of VMware expanded support for NVMe across PCIe storage, Fibre Channel, and RDMA to now include NVMe over TCP.
  - This SFSS component maps NVMe onto the TCP protocol to enable the transfer of data and commands between the VMware ESXi server and a target storage device.
- **PowerStore with NVMe/TCP:** PowerStore mid-range storage systems already include support for NVMe Flash drives and iSCSI, Fibre Channel, and NVMe-FC block protocols. The latest PowerStore release introduces support for NVMe/TCP to allow servers to access storage systems across a network fabric using the NVMe protocol.



# Software Defined Storage and Network

## Software Defined Storage and Network

## Software-Defined Storage

## Need for Software-Defined Storage

In a traditional data center, there are several challenges in provisioning and managing storage in an efficient and cost-effective manner. Some of the key challenges are:

- In traditional environments, the creation of complex IT silos in data centers leads to:
  - Management overhead
  - Increased costs
  - Poor resource utilization
- In data centers, critical functionality and management tied to storage system limits
  - Resource sharing
  - Automation
  - Standardization
- Traditional architecture makes it difficult to support:
  - Data growth
  - Scaling
  - Self-service

## Software-Defined Storage (SDS)

**Software-defined Storage** is storage infrastructure that is automated through software, which pools heterogeneous storage resources, and allocates them based on policy to match application needs.



- SDS abstracts heterogeneous storage systems and their underlying capabilities, and pools the storage resources.
- Storage capacity is dynamically and automatically allocated from the storage pools based on policies to match the needs of applications.
- Supports multiple types of storage systems and access methods.
  - Enables storing data on both storage systems and commodity disks.
  - Provides a unified external view of storage infrastructure.
- SDS enables organizations to build modern, hyperscale storage infrastructure in a cost-effective manner using standardized, commercial off-the-shelf components.

## Key Attributes of Software-Defined Storage

SDS transforms existing heterogeneous physical storage into a simple, extensible, and open virtual storage platform. The key attributes of software-defined storage are:

Attributes	Description
Storage abstraction and pooling <sup>57</sup>	Single large storage pool spanning across the underlying storage infrastructure.
Automated, policy-driven storage provisioning <sup>58</sup>	Dynamic composition of storage services based on application policies.

---

<sup>57</sup> SDS abstracts and pools storage resources across heterogeneous storage infrastructure. SDS software creates a single large storage pool with the underlying storage resources, from which several virtual storage pools are created. SDS decouples the storage control path from the data path. Applications connect to storage through the data path.

<sup>58</sup> A “storage service” is some combination of capacity, performance, protection, encryption, and replication. In the SDS model, storage services are dynamically composed from available resources. SDS uses application policies to create a “just-in-time” model for storage service delivery. Storage assets and capabilities are configured and assigned to specific applications only when they are needed. If the policy changes, the storage environment dynamically and automatically responds with the new requested service level.

## Software-Defined Storage

Unified management <sup>59</sup>	Single control point for the entire infrastructure.
Self-service <sup>60</sup>	Users self-provision storage services from a service catalog.
Open and extensible <sup>61</sup>	Integration of external interfaces and applications by using APIs.

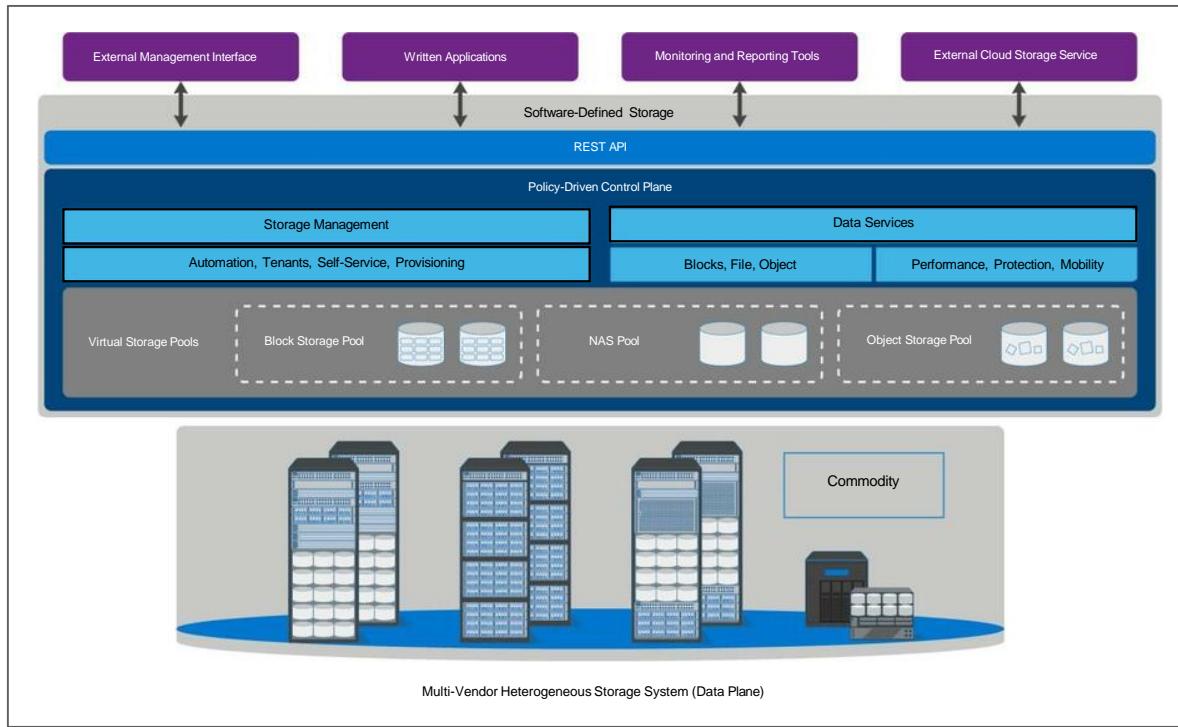
---

<sup>59</sup> SDS provides a unified storage management interface that provides an abstract view of the storage infrastructure. Unified management provides a single control point for the entire infrastructure across all physical and virtual resources.

<sup>60</sup> Resource pooling enables multi-tenancy, and automated storage provisioning enables self-service access to storage resources. Users select storage services from a self-service catalog and self-provision them.

<sup>61</sup> An SDS environment is open and easy to extend enabling new capabilities to be added. An extensible architecture enables integrating multi-vendor storage, and external management interfaces and applications into the SDS environment through the use of application programming interfaces (APIs).

## Software-Defined Storage Architecture



*Generic architecture of a software-defined storage environment.*

In SDS architecture, physical storage may be block-based, file-based, or object-based storage systems or commodity hardware.

- The fundamental component of the SDS environment is the policy-driven control plane, which manages and provisions storage.

## Software-Defined Storage

- The control plane is implemented through software that is called the “SDS controller<sup>62</sup>”.
- Users provision storage using data services, which may be block, file, or object services.

Key control plane functions are:

### Asset Discovery

- Controller automatically detects storage assets when they are added to the SDS environment.
- Examples of asset categories that can be discovered are:
  - Storage systems
  - Storage networks
  - Compute systems and clusters.
  - Data protection solutions

### Resource Abstraction and Pooling

An SDS controller exposes the storage infrastructure through a simplified model, hiding and handling details such as storage system and disk selection, LUN creation, LUN masking, and the differences between the storage systems.

SDS abstracts storage across the physical storage systems and manages individual components. This functionality enables administrators and users to treat storage as a large resource.

---

<sup>62</sup> The SDS controller is software that manages, abstracts, pools, and automates the physical storage systems into policy-based virtual storage pools.

## Service catalog and Self-service

- Administrator creates storage services and organizes them in a service catalog.
  - Services include block, file, and object data services.
  - Users place service requests through the user interface or a client software.
- SDS controller automates the provisioning of resources.

## Block Data Service

- Provides a block volume of required size, and performance and protection levels
- Examples of block services:
  - Create a block volume.
  - Delete a block volume.
  - Bind a block volume to compute.
  - Unbind a block volume from compute.
  - Mount a block volume.
  - Unmount a block volume
  - Expand a block volume.

## Benefits of Software-Defined Storage

The key benefits of software-defined storage are:

Benefits	Description
Simplified Storage Environment	<ul style="list-style-type: none"><li>Breaks down storage silos and their associated complexity.</li><li>Provides centralized management across all physical and virtual storage environments.</li></ul>
Operational Efficiency	<ul style="list-style-type: none"><li>Automated policy-driven storage provisioning improves quality of services, reduces errors, and lowers operational costs.</li><li>Provides faster streamlined storage provisioning, which enables new requests to be satisfied more rapidly.</li></ul>
Agility	<ul style="list-style-type: none"><li>Ability to deliver self-service access to storage through a service catalog provides agility and reduces time-to-market.</li></ul>
Reusing Existing Infrastructure	<ul style="list-style-type: none"><li>Supports multi-vendor storage systems and commodity hardware, which enables organizations to work with their existing infrastructure and protects the current investments of organizations.</li></ul>
Cloud Support	<ul style="list-style-type: none"><li>Enables an enterprise data center to connect to external cloud storage services for consuming services such as cloud-based backup, and disaster recovery.</li></ul>

## Knowledge Check

## Knowledge Check

### Knowledge Check

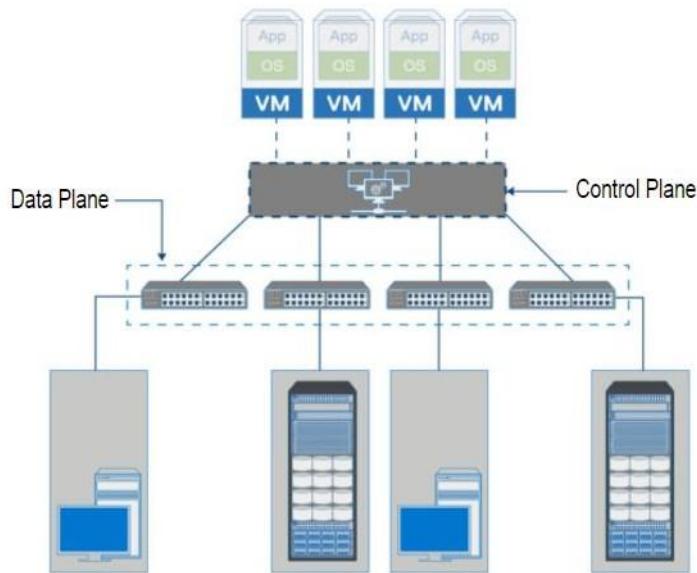
1. Match the following Software-defined storage attributes with their correct description.

A.Open and extensible	<u>B</u>	Single large storage pool spanning across the underlying storage infrastructure.
B.Storage abstraction and pooling	<u>C</u>	Single control point for the entire infrastructure.
C.Unified management	<u>A</u>	Integration of external interfaces and applications by using APIs.
D.Self-service	<u>D</u>	Users self-provision storage services from a service catalog.

## Software-Defined Networking (SDN)

## Software-Defined Networking

## Introduction to Software-Defined Networking



SDN is an approach to abstract and separate the control plane functions from the data plane functions.

Instead of the integrated control functions at the network components level, the software external to the components takes over the control functions.

The software runs on a compute system or a stand-alone device and is called network controller.

- Controller gathers configuration information from network components.
- Controller provides instructions to data plane.

### Software-Defined Networking Benefits

Software-defined networking benefits are:

#### Centralized Control



- Provides a single point of control for the entire network infrastructure that may span across data centers.
- Centralized control plane provides the programming logic for transferring the network traffic, which can be uniformly and quickly applied across the network infrastructure.
- Programming logic can be upgraded centrally to add new features based on application requirements.

#### Policy-based Automation



- Many hardware-based network management operations such as zoning can be automated.

- Management operations may be programmed in the network controller that is based on business policies and best practices.
- Reduces the need for manual operations that are repetitive, error-prone, and time-consuming.
- Helps to standardize the management operations.

### Agile Management

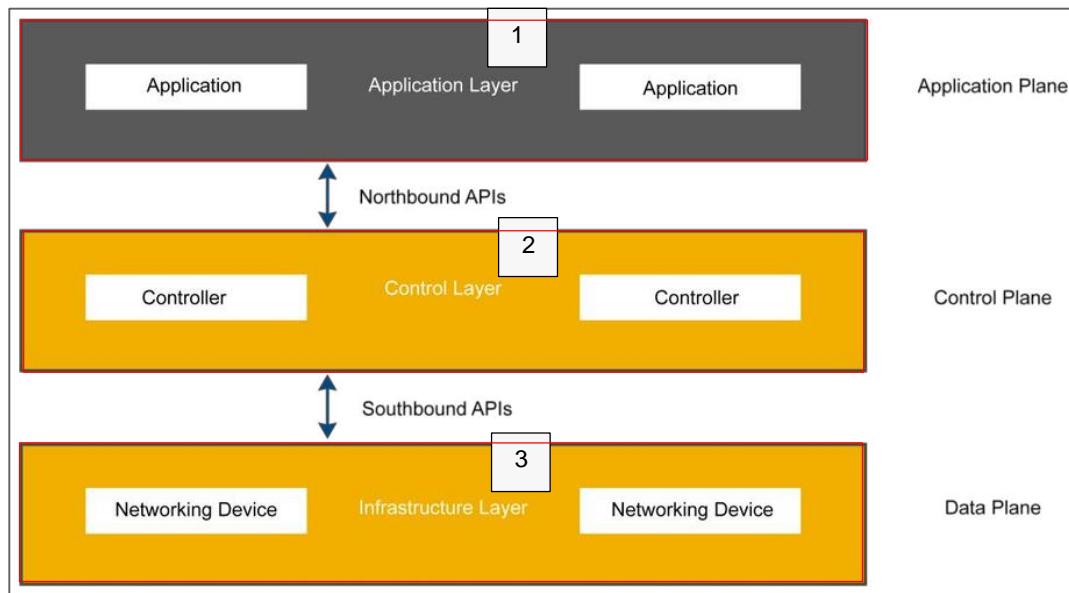


- Network controller usually provides a management interface that includes a limited and standardized set of management functions.
- Management functions are available in a simplified form, abstracting the underlying operational complexity.
- Makes it easier to configure a network infrastructure and to modify the network configuration to respond to changing application requirements.

### Software-Defined Networking Architecture

The architecture of SDN consists of three layers along with APIs<sup>63</sup> in between to define the communication.

Software-defined Architecture.



**1:** Consists of applications and services such as business applications, and analytics that define the network behavior through policies and also define the requirements. It communicates the requirements through the APIs to the control layer. This layer forms the application plane of the SDN architecture.

---

<sup>63</sup> APIs are referred as northbound interfaces and southbound interfaces.

Northbound interfaces define the communications between the controller and application layer. Southbound interfaces define the communications between the control and infrastructure layer.

**2:** Consists of controllers and acts as a brain of the SDN architecture. It is responsible for making decisions such as how the packets should be forwarded based on the requirements, and relays the decisions to the networking devices (data plane) for execution. It also extracts the information about the network from the data plane and communicates it to the application layer. This layer forms the control plane.

**3:** Consists of networking devices such as switches and routers. It is responsible for handling data packets such as forwarding or dropping of packets and handling the devices. This layer forms the data plane and performs actions based on the instructions received.

### Software-Defined Networking Use Case

#### Data Center Security



- Security against lateral movements.
- Visibility of trends using analytics such as switch data.
- Security policies and control for each workload.

Click here<sup>64</sup> to understand more about data center security.

---

<sup>64</sup> Protecting information is a strategic necessity for organizations. With SDN, organizations protect data through embedded security, to prevent credential stealing and computer infiltration for both the physical and virtual layers. It enables visibility of trends using analytics available that offer insight into switch traffic. Micro-segmentation feature of SDN lets organizations define security policies and controls for each workload based on dynamic security groups. This process helps to ensure immediate responses to threats inside the data center.

### Automation



- Automated network provisioning.
- Programmatically control the entire network environment.

Click [here<sup>65</sup>](#) to understand more about automation.

---

<sup>65</sup> Many organizations cannot change their networks fast enough to keep up with new applications and workloads. With SDN, organizations can bring up workloads in seconds or minutes using automated network provisioning. There is no need to make major revisions to the physical network every time the organization introduces an application or service. Changes can be quickly made through software and require few, if any, cabling updates. IT can programmatically create, snapshot, store, move, delete, and restore entire networking environments with simplicity and speed. This automation of networking tasks benefits both new application deployments as well as changes to existing applications in the IT infrastructure.

### Business Continuity



- Hybrid cloud initiatives.
- Disaster recovery.

Click [here<sup>66</sup>](#) to understand more about business continuity.

---

<sup>66</sup> SDN also simplifies and accelerates private and hybrid cloud initiatives. Organizations can rapidly develop, automatically deliver, and manage all their enterprise applications, whether they reside on-premises or off-premises, from a single unified platform. IT can easily replicate entire application environments to remote data centers for disaster recovery. It can also move them from one corporate data center to another or deploy them into a hybrid cloud environment, without disrupting the applications or touching the physical network.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Which layer in the software-defined networking architecture is responsible to make the decisions like packet forwarding?
  - a. Application and control layer
  - b. Control layer
  - c. Infrastructure and application layer
  - d. Infrastructure layer

## Concepts in Practice

## Concepts in Practice

### Dell EMC PowerFlex

- Is a fully integrated, preconfigured, and validated hyperconverged infrastructure appliance that integrates PowerFlex virtualization software with Dell EMC PowerEdge servers.
- Is used in a hyperconverged or server SAN architecture, heterogeneous virtualized environments, and high-performance databases.
- Provides large storage capacity and scalability.
- Manages compute and storage resources together or independently depending on business needs.
- Provides enterprise-grade data protection, multitenant capabilities, and add-on enterprise features such as quality of service (QoS), thin provisioning, and snapshots.



### Dell VxFlex OS

- Creates a server and IP-based SAN from direct-attached server storage.

- Combines HDDs, SSDs, and PCIe flash cards to create a virtual pool of block storage with varying performance tiers.
- Can deliver millions of IOPS at consistent submillisecond response times.



## VMware NSX-T

- Network virtualization platform for Software-Defined Data Center (SDDC) architectures.
- Virtual networks are programmatically provisioned and managed, independent of underlying hardware.
- Enables a library of logical networking elements, such as logical switches, routers, firewalls, and load balancers.

## Business Continuity

## Business Continuity

## Business Continuity Overview

## Business Continuity



**Business continuity (BC)** is a process that prepares for, responds to, and recovers from a system outage that can adversely affect business operations.

- BC enables continuous availability of information and services in the event of failure.
- BC involves various proactive and reactive countermeasures.
- It is important to automate BC processes to reduce manual intervention.
  - To maximize application and information availability.
- Goal of BC solutions are to ensure information availability.
  - Automation is the key to minimize any downtime.

For example: A natural disaster causes an electrical outage to a data center. Proper business continuity planning will ensure that there is adequate battery backup to maintain the systems until the backup generators begin to operate. In the case of mission critical applications, the business continuity plan should be able to transfer the workload to a different datacenter.

### Notes:

## Business Continuity Overview

Business continuity (BC) is a set of processes that includes all activities that a business must perform to mitigate the impact of planned and unplanned downtime. BC entails preparing for, responding to, and recovering from a system outage that adversely affects business operations. It describes the processes and procedures an organization establishes to ensure that essential functions can continue during and after a disaster.

Business continuity prevents interruption of mission-critical services, and reestablishes the impacted services as swiftly and smoothly as possible by using an automated process. BC involves proactive measures such as business impact analysis, risk assessment, building resilient IT infrastructure, deploying data protection solutions (backup and replication). It also involves reactive countermeasures such as disaster recovery.

In a modern data center, policy-based services can be created that include data protection through the self-service portal. Consumers can select the class of service that best meets their performance, cost, and protection requirements on demand. Once the service is activated, the underlying data protection solutions that are required to support the service are automatically invoked to meet the required data protection.

## Information Availability

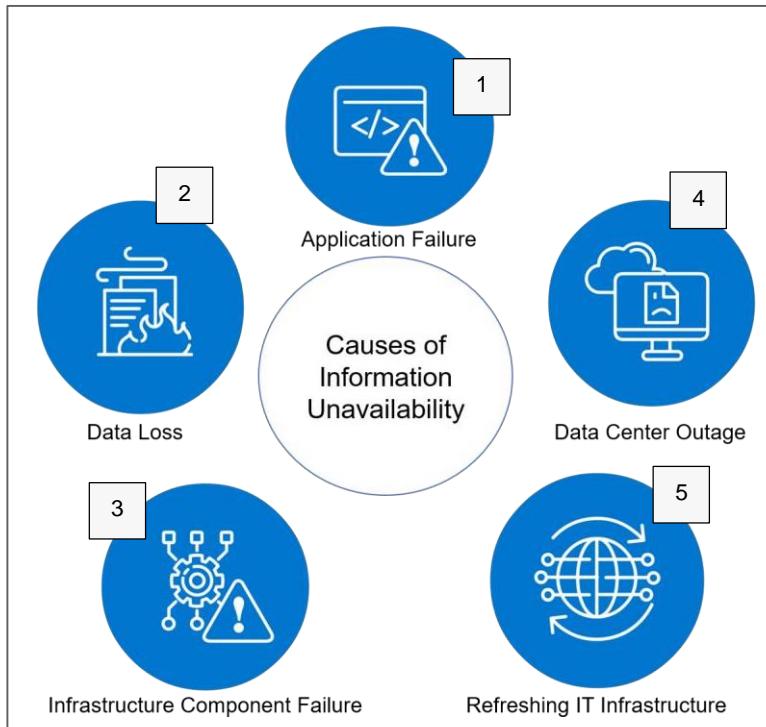
## Business Continuity Overview

**Information availability** is the ability of an IT infrastructure to function according to business requirements and customer expectations, during its specified time of operation.

Information Availability can be defined in terms of:

	<p><b>Accessibility:</b> Information should be accessible to the right user when required.</p>
	<p><b>Reliability:</b> Information should be reliable and correct in all aspects. It is “the same” as what was stored and there is no alteration or corruption to the information.</p>
	<p><b>Timelines:</b> Defines the time window (a particular time of the day, week, month, and year as specified) during which information must be accessible. For example: if online access to an application is required between 8:00 am and 10:00 pm each day, any disruption to data availability outside of this time slot is not considered to affect timeliness.</p>

## Causes of Information Unavailability



**1:** Due to catastrophic exceptions caused by bad logic.

**2:** Multiple drive failures in a RAID group.

**3:** A network switch failure without any redundant paths.

**4:** Due to power failure or disaster.

**5:** Scheduled maintenance requiring downtime.

### Notes:

Data center failure due to disaster (natural or man-made disasters such as flood, fire, earthquake, and so on) is not the only cause of information unavailability. Poor application design or resource configuration errors can lead to information unavailability. For example, if the database server is down for some reason, then the data is inaccessible to the consumers, which leads to IT service outage.

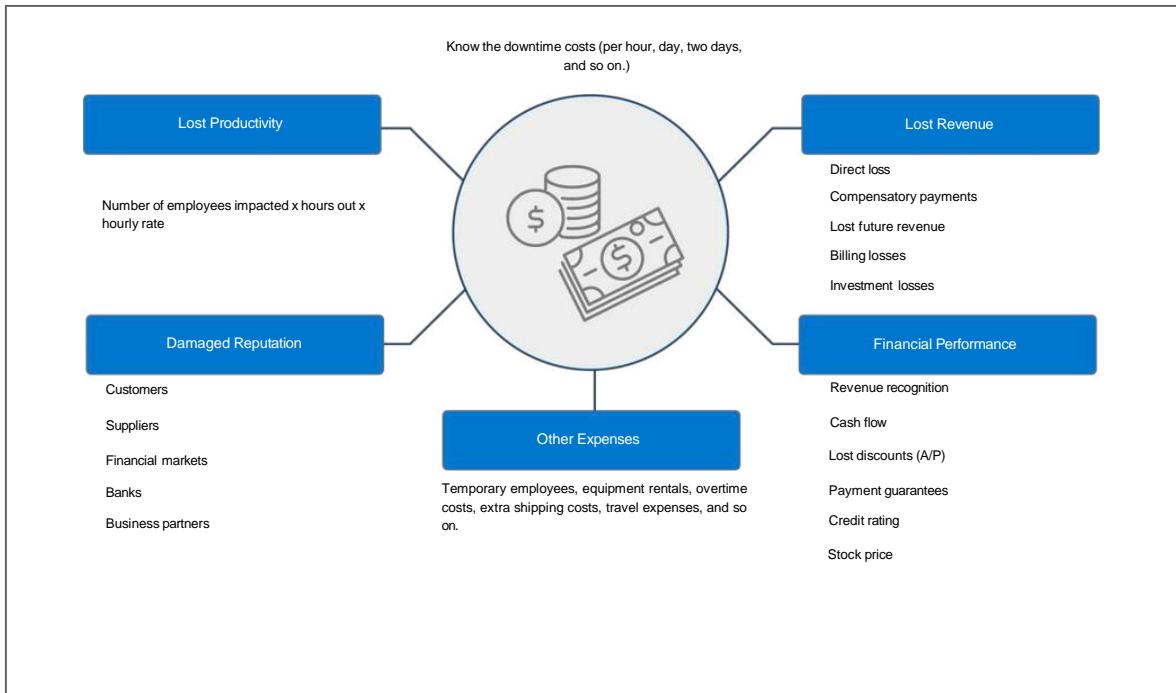
## Business Continuity Overview

Even the unavailability of data due to several factors (data corruption and human error) leads to outage. The IT department is routinely required to take on activities such as refreshing the data center infrastructure, migration, running routine maintenance, or even relocating to a new data center. Any of these activities can have its own significant and negative impact on information availability.

**Note:** In general, the outages can be broadly categorized into planned and unplanned outages.

- Planned outages may include installation and maintenance of new hardware, software upgrades or patches, performing application and data restores, facility operations (renovation and construction), and migration.
- Unplanned outages include failure caused by human errors, database corruption, failure of physical and virtual components, and natural or human-made disasters.

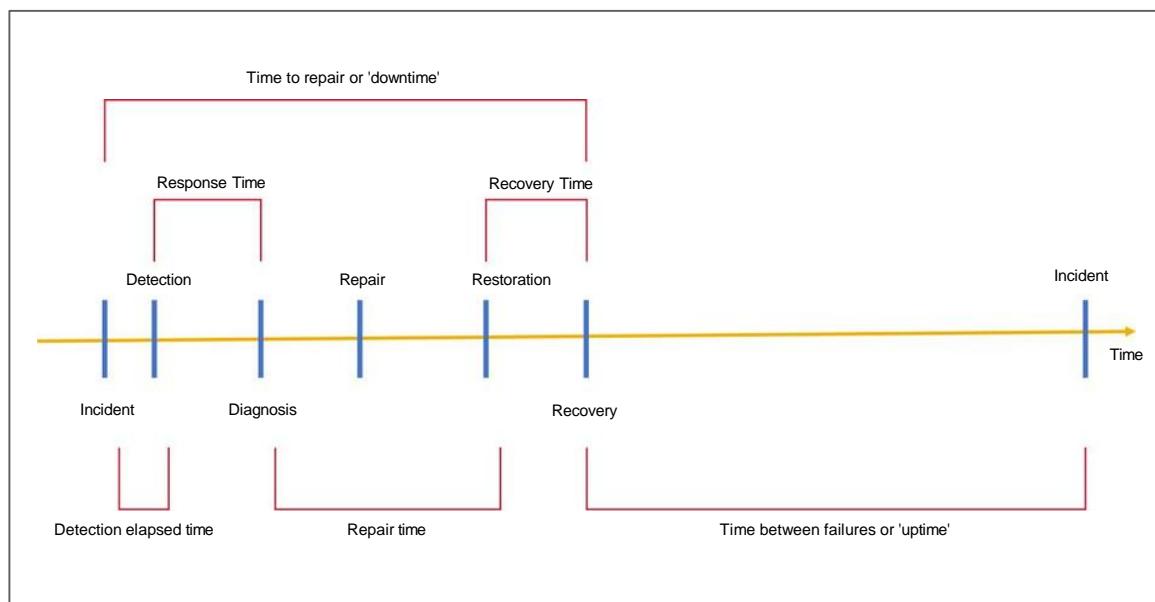
## Impact of Information Unavailability



### Measurement of Information Availability

Information availability relies on the availability of both physical and virtual components of a data center. The failure of these components might disrupt information availability.

The component's ability can be restored by performing various external corrective actions, such as a manual reboot, a repair, or replacement of the failed component(s). Proactive risk analysis, performed as part of the BC planning process, considers the component failure rate and average repair time, which are measured by MTBF and MTTR.



**MTBF:** Average time available for a system or component to perform its normal operations between failures

- **MTBF** = Total uptime / Number of failures

**MTTR:** Average time required to repair a failed component

- **MTTR** = Total downtime / Number of failures

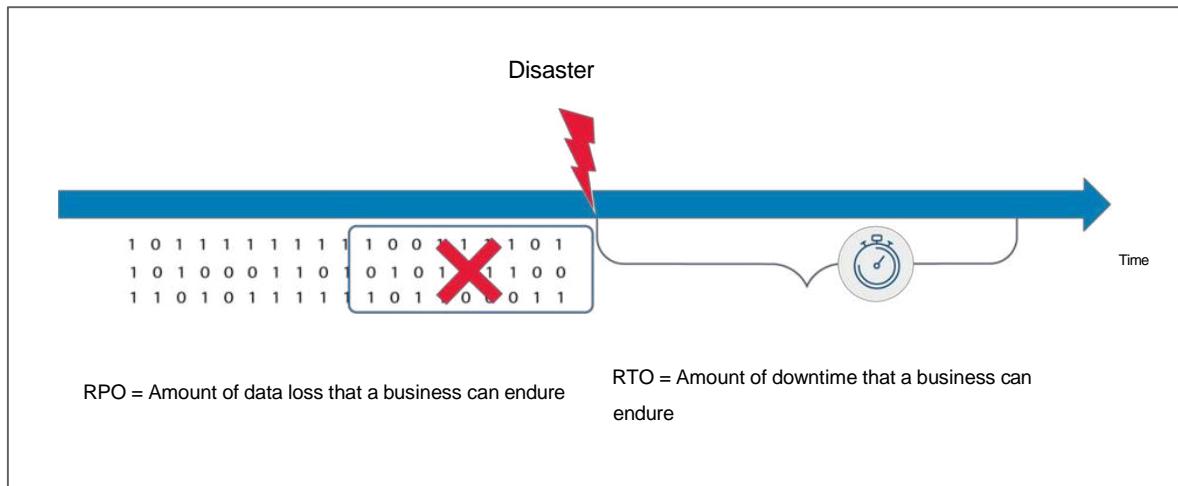
---

**IA = MTBF / (MTBF + MTTR) or IA = Uptime / (Uptime + Downtime)**

---

### RPO and RTO

Recovery Point Objectives (RPO)	Recovery Time Objectives (RTO)
Point-in-time to which data must be recovered.	Time within which systems and applications must be recovered.



#### Notes:

When designing an information availability strategy for an application or a service, organizations must consider two important parameters that are closely associated with recovery.

- **Recovery Point Objective:** RPO is the point-in-time to which data must be recovered after an outage. It defines the amount of data loss that a business can endure. Based on the RPO, organizations plan for the frequency with which a backup or replica must be made. For example, if the RPO of a particular business application is 24 hours, then backups are created every midnight. The corresponding recovery strategy is to restore data from the set of last backups. An organization can plan for an appropriate BC solution on the basis of the RPO it sets.
- **Recovery Time Objective:** RTO is the time within which systems and applications must be recovered after an outage. It defines the amount of

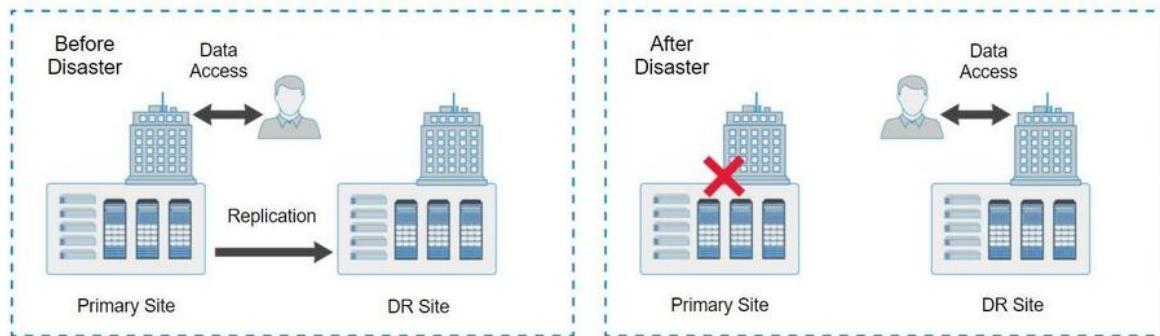
## Business Continuity Overview

downtime that a business can endure and survive. Based on the RTO, an organization can decide which BC technology is best suited. The more critical the application, the lower the RTO should be.

Both RPO and RTO are counted in minutes, hours, or days and are directly related to the criticality of the IT service and data. Usually, the lower the RTO and RPO, the higher is the cost of a BC solution or technology.

### Disaster Recovery

**Disaster recovery** involves a set of policies and procedures for restoring IT infrastructure, including data access, after a natural or human-induced disaster occurs.

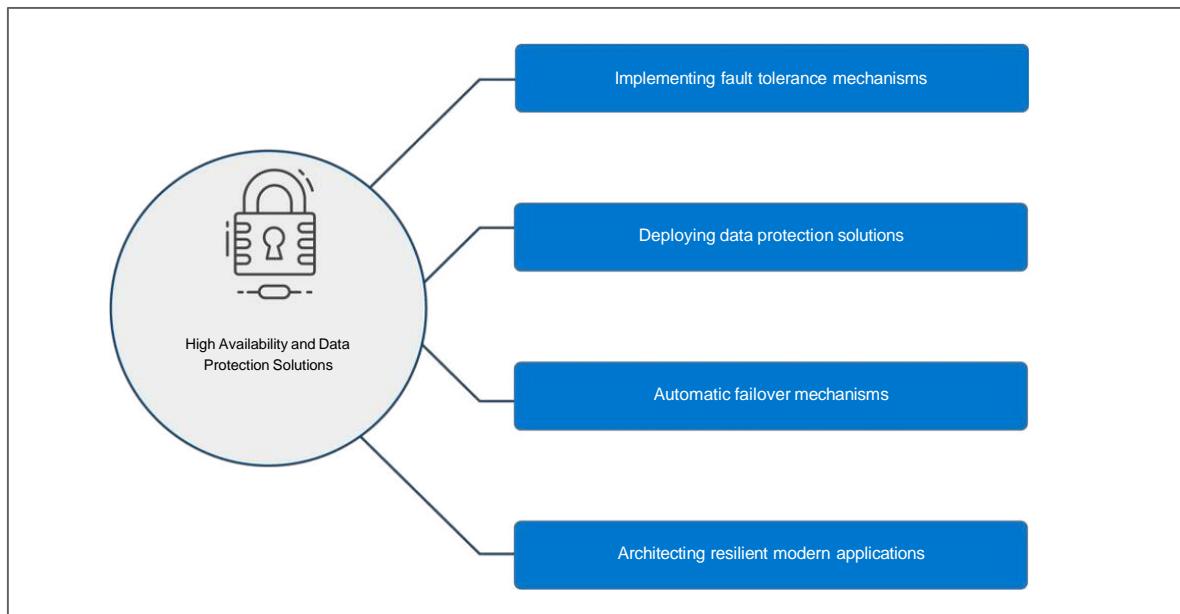


#### Notes:

The fundamental principle of DR is to maintain a secondary data center or site, called a DR site. The primary data center and the DR data center should be located in different geographical regions to avoid the impact of a regional disaster. The DR site must house a complete copy of the production data. Commonly, all production data is replicated from the primary site to the DR site either continuously or periodically. A backup copy can also be maintained at the DR site. Usually, the IT infrastructure at the primary site is unlikely to be restored within a short time after a catastrophic event.

Organizations often keep their DR site ready to restart business operations if there is an outage at the primary data center. This may require the maintenance of a complete set of IT resources at the DR site that matches the IT resources at the primary site. Organization can either build their own DR site, or they can use cloud to build DR site.

### Business Continuity Technology Solutions



#### Notes:

With the aim of meeting the required information and service availability, the organizations should build a resilient IT infrastructure. Building a resilient IT infrastructure requires the following high availability and data protection solutions:

- Deploying redundancy at both the IT infrastructure component level and the site level to avoid single point of failure
- Deploying data protection solutions such as backup, replication, migration, and archiving
- Automatic failover mechanism is one of the important methods as well. It is one the efficient and cost effective way to ensure HA. For example, scripts can be defined to bring up a new VM automatically when the current VM stops responding or goes down.
- Architecting resilient modern applications

For example: when a disaster occurred at one of the data centers of an organization, the BC triggers the DR process. This process typically involves both manual and automated procedure to reactivate the service (application) at a functioning data center. This reactivation of service requires the transfer of

## Business Continuity Overview

application users, VMs, data, and services to the new data center. This process involves the use of redundant infrastructure across different geographic locations, live migration, backup, and replication solutions.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Which defines the amount of data loss that a business can endure?

- a. RTO
- b. RPO
- c. MTBF
- d. MTTR

## Fault Tolerance Infrastructure

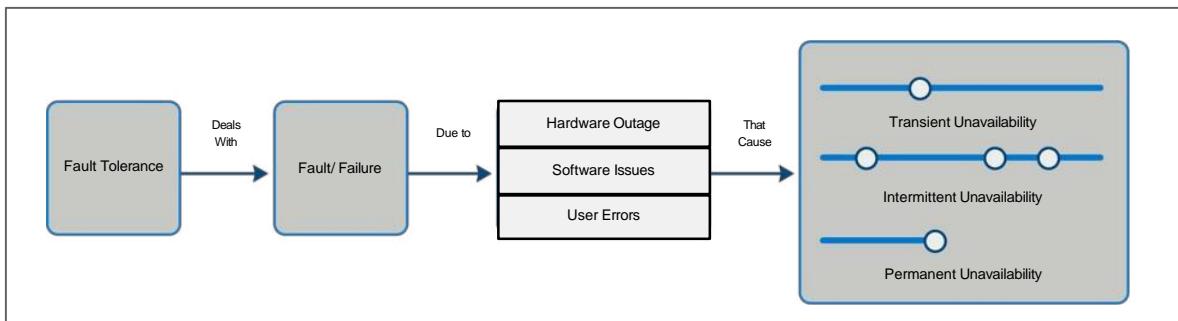
## Fault Tolerance Infrastructure

## Fault Tolerance IT Infrastructure Overview

**Fault Tolerance** is the ability of an IT system to continue functioning in the event of a failure.

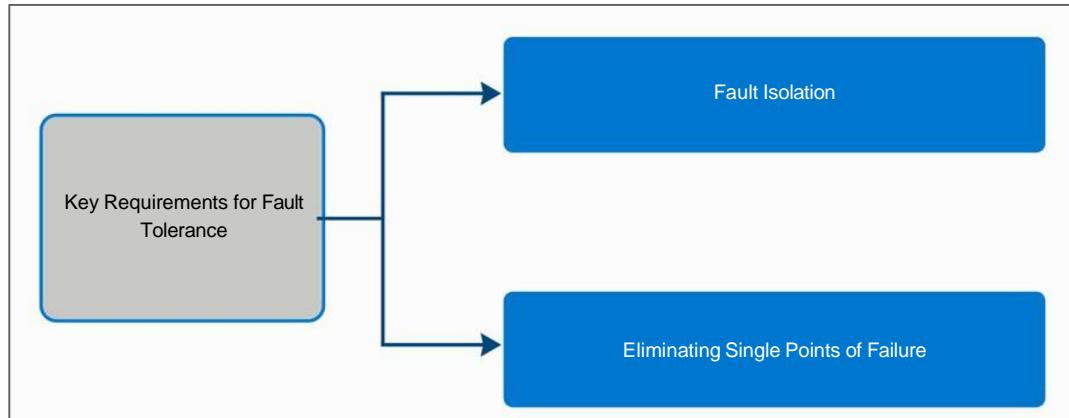
A fault may cause a complete outage of a component or cause a faulty component to run but only to produce incorrect or degraded output. The common reasons for a fault are: hardware defect, software bug, and administrator/user errors.

Fault tolerance ensures that a single fault or failure does not make an entire system or a service unavailable. It protects an IT system or a service against various types of unavailability.



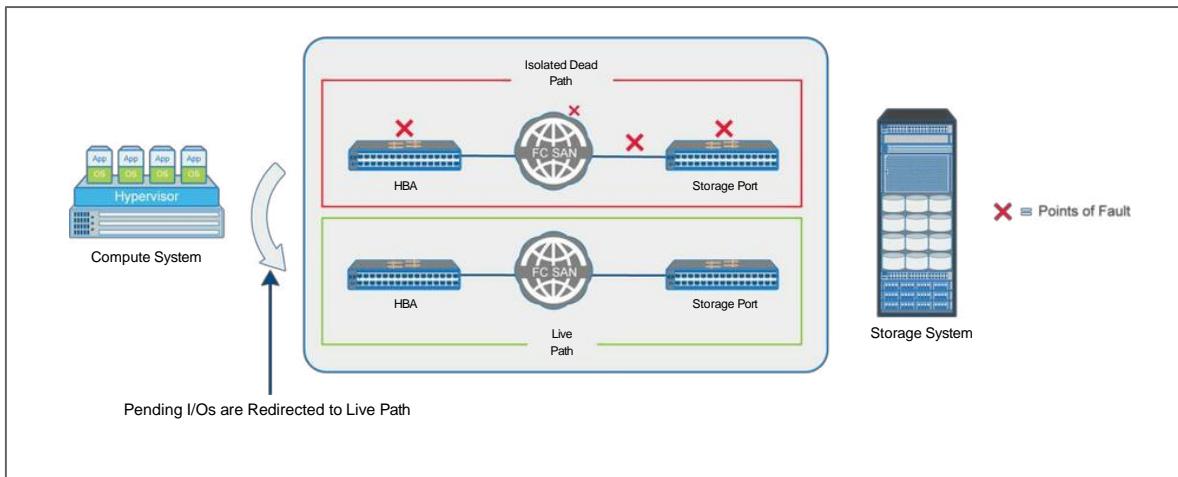
### Key Requirements for Fault Tolerance

Fault tolerant IT infrastructure meets two key requirements: fault isolation and eliminating single points of failure (SPOF).



## Fault Isolation

Fault isolation contains the scope of a fault so that the other areas of a system are not impacted by the fault. It does not prevent failure of a component but ensures that the failure does not impact the overall system.

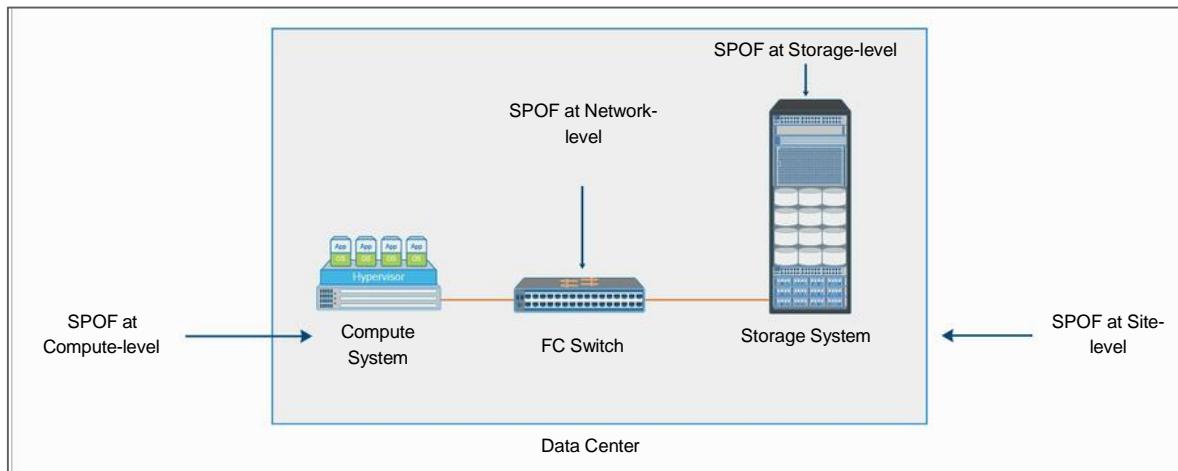


The example represents two I/O paths between a compute system and a storage system. The compute system uses both paths to send I/O requests to the storage system. If an error or fault occurs on a path causing a path failure, the fault isolation mechanism present in the environment automatically detects the failed path. The failed path is marked as a dead path to avoid sending pending I/Os through it. All pending I/Os are redirected to the live path. This fault isolation avoids time-out and the retry delays.

### Single Points of Failure

**Single Points of Failure (SPOF)** refers to any individual component or aspect of an infrastructure whose failure can make the entire system or service unavailable.

Single points of failure may occur at infrastructure component-level and site-level (data center).



The image provides an example where various IT infrastructure components, including the compute system, VM instance, network devices, storage, and site itself, become a single point of failure. Assume that a web application runs on a VM instance and it uses a database server which runs on another VM to store and retrieve application data. If the database server is down then the application would not be able to access the data and in turn would impact the availability of the service.

## Eliminating Single Points of Failure

Single points of failure can be avoided by implementing fault tolerance mechanisms such as redundancy.

- Implement redundancy at component level
  - Compute
  - Network
  - Storage
- Implement multiple availability zones
  - Avoid single points of failure at data center (site) level.

**Notes:**

Highly available infrastructures are typically configured without single points of failure to ensure that individual component failures do not result in service outages. The general method to avoid single points of failure is to provide redundant components for each necessary resource, so that a service can continue with the available resource even if a component fails.

Organizations may also create multiple availability zones to avoid single points of failure at data center level. Usually, each zone is isolated from others, so that the failure of one zone would not impact the other zones. It is important to have high availability mechanisms that enable automated application/service failover within and across the zones if there is a component failure or disaster.

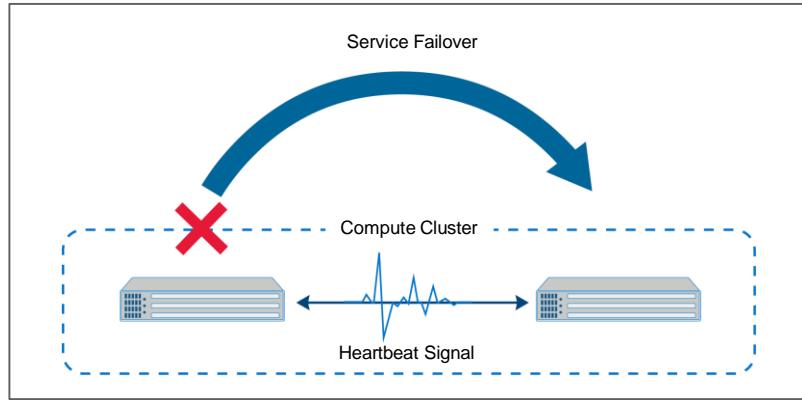
N+1 redundancy with active/active component configuration is also available. In such cases, all the component remains active. For example, if an active/active configuration is implemented at the site level and then a service is fully deployed in both the sites. The load for this service is balanced between the sites. If one of the sites is down, the available site would manage the service operations and manage the workload.

## Eliminating Single Points of Failure: Additional Information



*Click [here](#) to understand the eliminating single points of failure*

## Compute Clustering

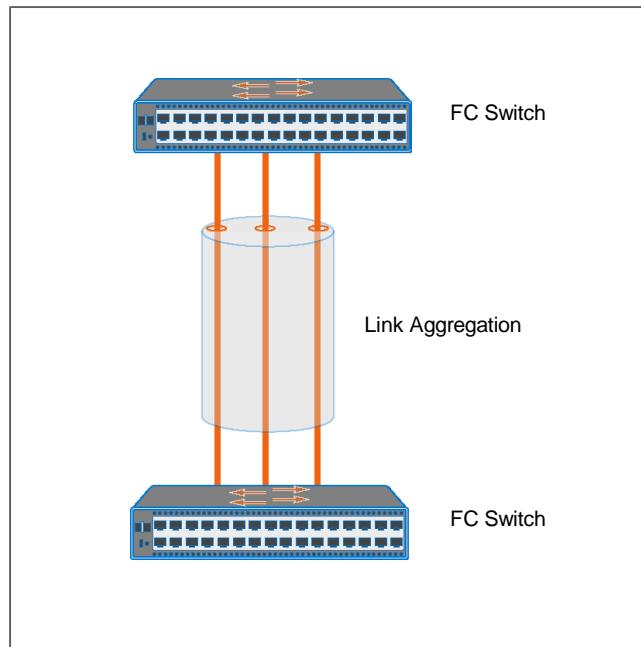


- Two or more compute systems/hypervisors are clustered to provide high availability and load balancing.
- Service running on a failed compute system moves to another compute system.
  - Heartbeat mechanism determines the health of compute systems in a cluster.
- Two common clustering implementations are:
  - Active/active
  - Active/passive

## Network Fault Tolerance Mechanisms

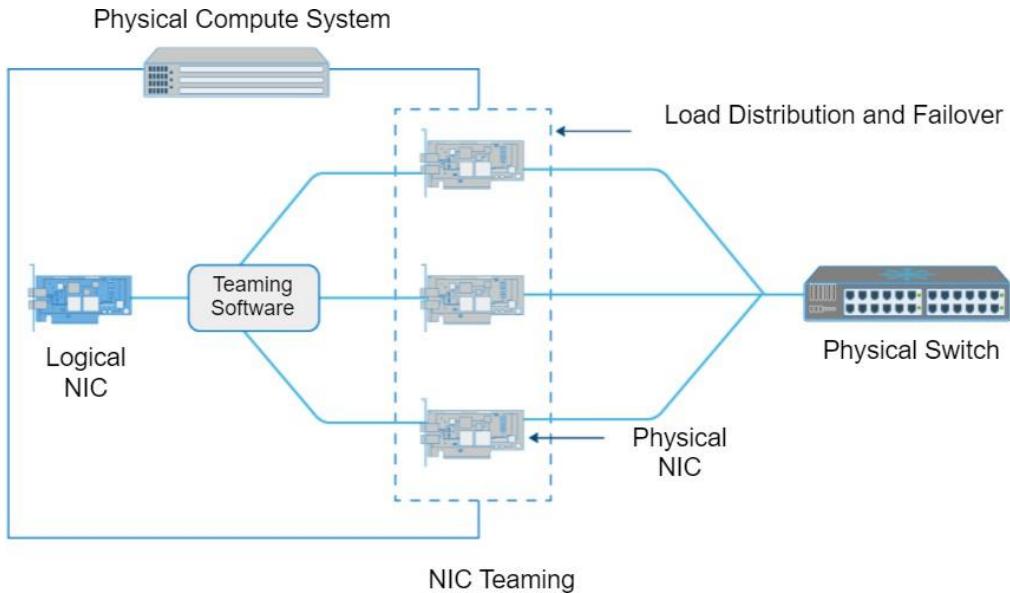
A short-time network interruption could impact plenty of services running in a data center environment. So, the network infrastructure must be fully redundant and highly available with no single points of failure. The following techniques provide fault tolerance against a failure:

### Link Aggregation



- Combines links between two switches and also between a switch and a node.
- Enables network traffic failover in the event of a link failure in the aggregation.

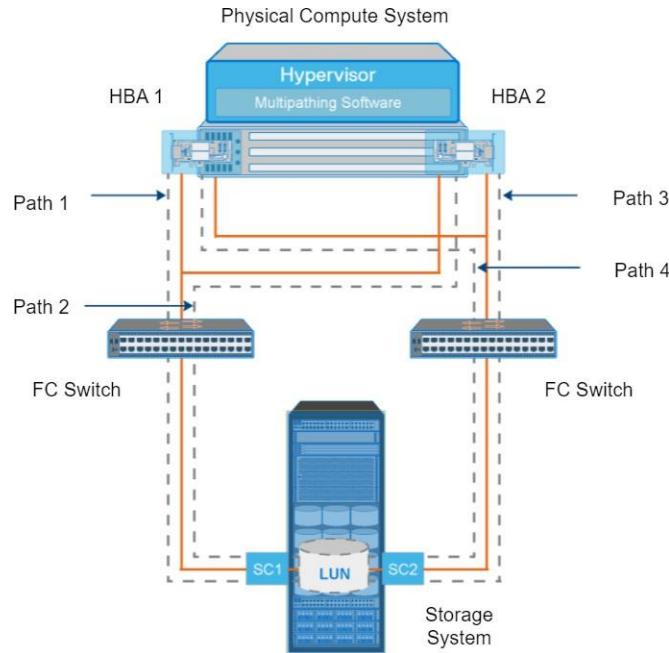
## NIC Teaming



- Groups network interface cards (NICs) so that they appear as a single logical NIC to the operating system or hypervisor.
- Provides network traffic failover in the event of a NIC/link failure.
- Distributes network traffic across NICs.

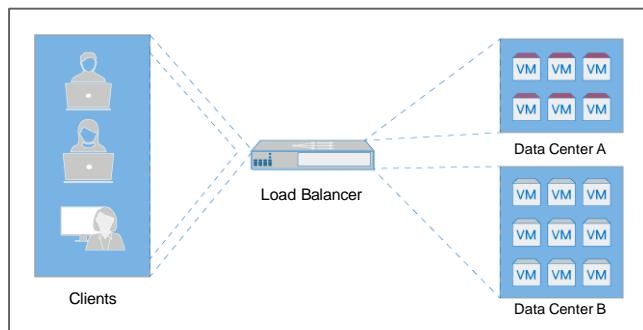
## Fault Tolerance Infrastructure

### Multipathing



- Enables a compute system to use multiple paths for transferring data to a LUN.
- Enables failover by redirecting I/O from a failed path to another active path.
- Performs load balancing by distributing I/O across active paths.

### Elastic Load Balancing



- Enables dynamic distribution of applications I/O traffic.
- Dynamically scales resources (VM instances) to meet traffic demands.
- Provides fault tolerance capability by detecting the unhealthy VM instances and automatically redirects the I/Os to other healthy VM instances.

## Storage Fault Tolerance Mechanisms

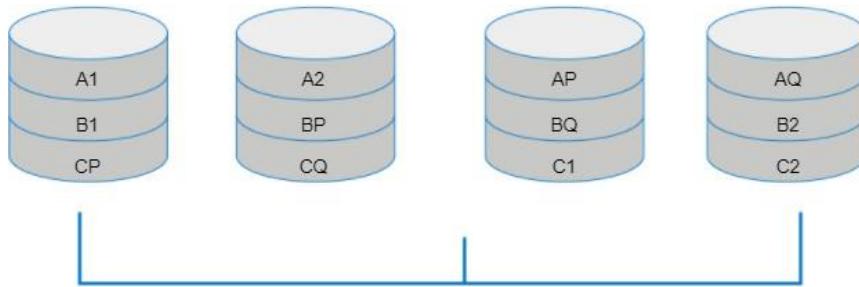
Data centers comprise storage systems with a large number of disk drives and solid state drives. The failure of these drives could result in data loss and information unavailability.

The following techniques provide data protection in the event of drive failure:

### RAID

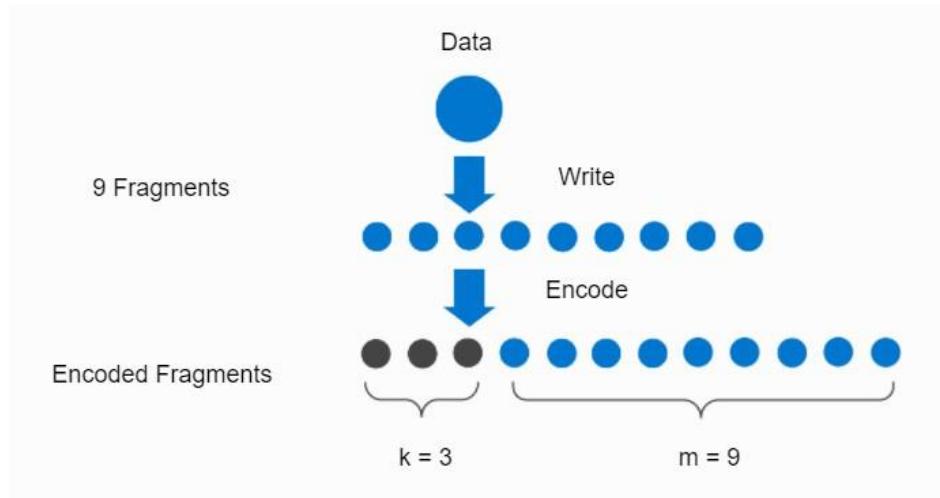
Provides data protection against one or two drive failures.

- RAID is a technique that combines multiple drives into a logical unit that is called a RAID set. Nearly all RAID implementation models provide data protection against drive failures.
- The illustration provides an example of RAID 6 (dual distributed parity), where data is protected against two disk failures. The data is striped across the disk with dual parity, for example as shown in the figure below the data "A" is striped across four disks (A1, A2 are data where as Ap and Aq are parity).



RAID 6 - Dual Distributed Parity

## Erasure Coding



- Provides space-optimal data redundancy to prevent data loss against multiple disk drive failures.
  - A set of  $n$  disks is divided into  $m$  disks to hold data and  $k$  disks to hold coding information.
  - Coding information is calculated from data.

The image illustrates an example of dividing data into nine data segments ( $m = 9$ ) and three coding fragments ( $k = 3$ ). The maximum number of drive failures tolerated in this example are three. Erasure coding offers higher fault tolerance (tolerates  $k$  faults) than replication with less storage cost.

## Dynamic Disk Sparing

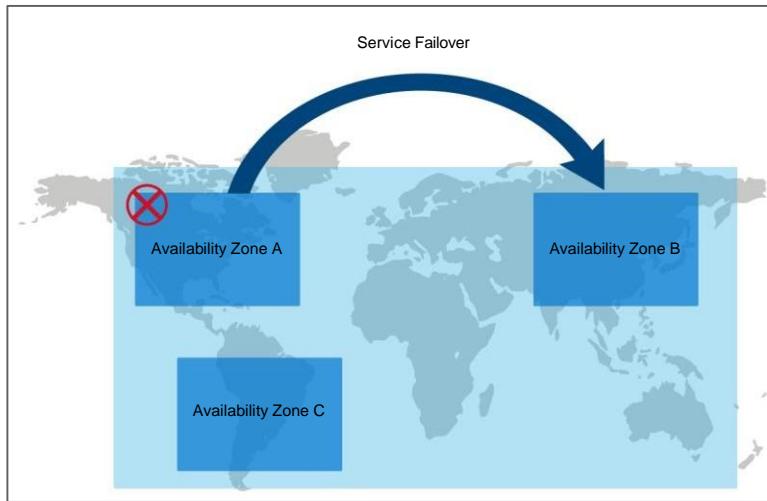
- Automatically replaces a failed drive with a spare drive to protect against data loss.
- Multiple spare drives can be configured to improve availability.
- When the recoverable error rates for a disk exceed a predetermined threshold, the disk subsystem tries to copy data from the failing disk to the spare drive automatically.

## Cache Protection - Mirroring

Any kind of cache failure will cause loss of data that is not yet committed to the storage drive. This risk of losing uncommitted data held in cache can be mitigated using cache mirroring.

- Each write to cache is held in two different memory locations on two independent memory cards.
- If a cache failure occurs, the write data will still be safe in the mirrored location and can be committed to the storage drive.

### Fault Tolerance at Site-Level – Availability Zones



- Availability zone is a location with its own set of resources and isolated from other zones.
- Availability zones, although isolated from each other, are connected through low-latency network links.
- In the event of a zone outage, services can failover to another zone.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Which fault tolerance mechanism provides space-optimal data redundancy to prevent data loss against multiple disk drive failures?
  - a. Erasure Coding
  - b. Dynamic Disk Sparing
  - c. Link Aggregation
  - d. Multipathing

## Concepts in Practice

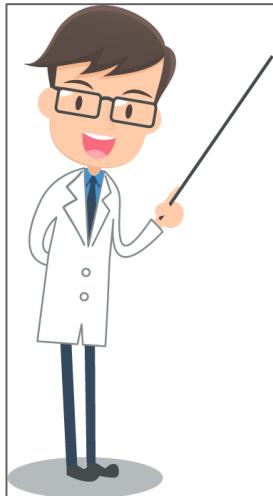
## Concepts in Practice

### Dell EMC PowerPath

- Dell EMC PowerPath is a family of software products that ensures consistent application availability and performance across I/O paths on physical and virtual platforms.
- PowerPath provides automated path management and tools that enable you to satisfy aggressive service-level agreements without investing in additional infrastructure.
- PowerPath includes PowerPath Migration Enabler for non-disruptive data migrations and PowerPath Viewer for monitoring and troubleshooting I/O paths.

## Exercise - Business Continuity

## Exercise: Information Availability



### Scenario

A system has three components and requires all three to be operational from 8 am to 8 pm, Monday to Friday. In a given week, failure of component 2 occurs as follows:

- Monday = 9 am to 12 pm
- Tuesday = No failure
- Wednesday = 5 pm to 8 pm
- Thursday = 4 pm to 7 pm
- Friday = 5 pm to 6 pm
- Saturday = 8 am to 1 pm

### Deliverables

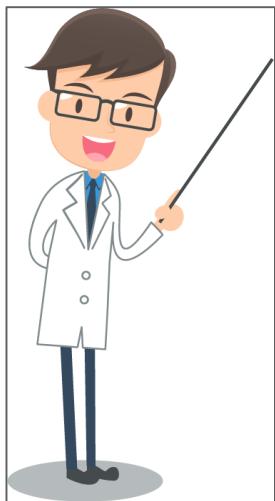
Calculate the availability of component 2.

### Solutions

- Availability is calculated as: system uptime / (system uptime + system downtime).
  - System uptime / (system uptime + system downtime).
- System downtime = 3 hours on Monday + 3 hours on Wednesday + 3 hours on Thursday + 1 hour on Friday = 10 hours.
  - We do not need to consider downtime on Saturday because component 2 is not required to be operational on weekends.
- System uptime = total operational time – system downtime, which is:
  - 60 hours – 10 hours, which is 50 hours.
- Availability (%) =  $(50 / 60) \times 100 = 83.3\%$ .

## Exercise - Business Continuity

### Exercise: MTBF and MTTR



#### Scenario

A system has three components and requires all three to be operational 24 hours/day from Monday to Friday. Failure of component 1 occurs as follows:

- Monday = No failure
- Tuesday = 5 am to 7 am
- Wednesday = No failure
- Thursday = 4 pm to 8 pm
- Friday = 8 am to 11 am

#### Deliverables

Calculate the MTBF and MTTR of component 1.

#### Solutions

MTBF is calculated as: total uptime / number of failures.

- Total downtime = 2 hours on Tuesday + 4 hours on Thursday + 3 hours on Friday = 9 hours.
- Total uptime =  $(5 \times 24) - 9 = 111$  hours.
- MTBF =  $111 / 3 = 37$  hours.

MTTR is calculated as: total downtime / number of failures.

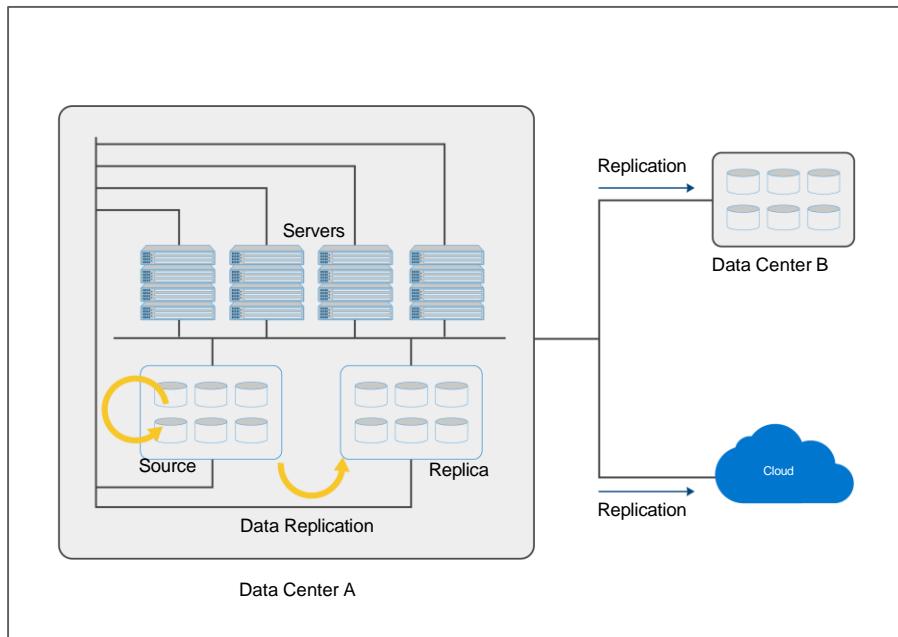
- Total downtime = 2 hours on Tuesday + 4 hours on Thursday + 3 hours on Friday = 9 hours.
- MTTR = 9 hours / 3 = 3 hours.

## Data Protection

## Data Protection

## Data Replication

## Data Replication Overview



### ***Data replication across different locations***

**Replication** is a process of creating an exact copy (replica) of the data to ensure business continuity when there is a local outage or disaster.

- Replicas<sup>67</sup> are used to restore and restart operations when there is data loss.
- Data can be replicated to one or more locations.

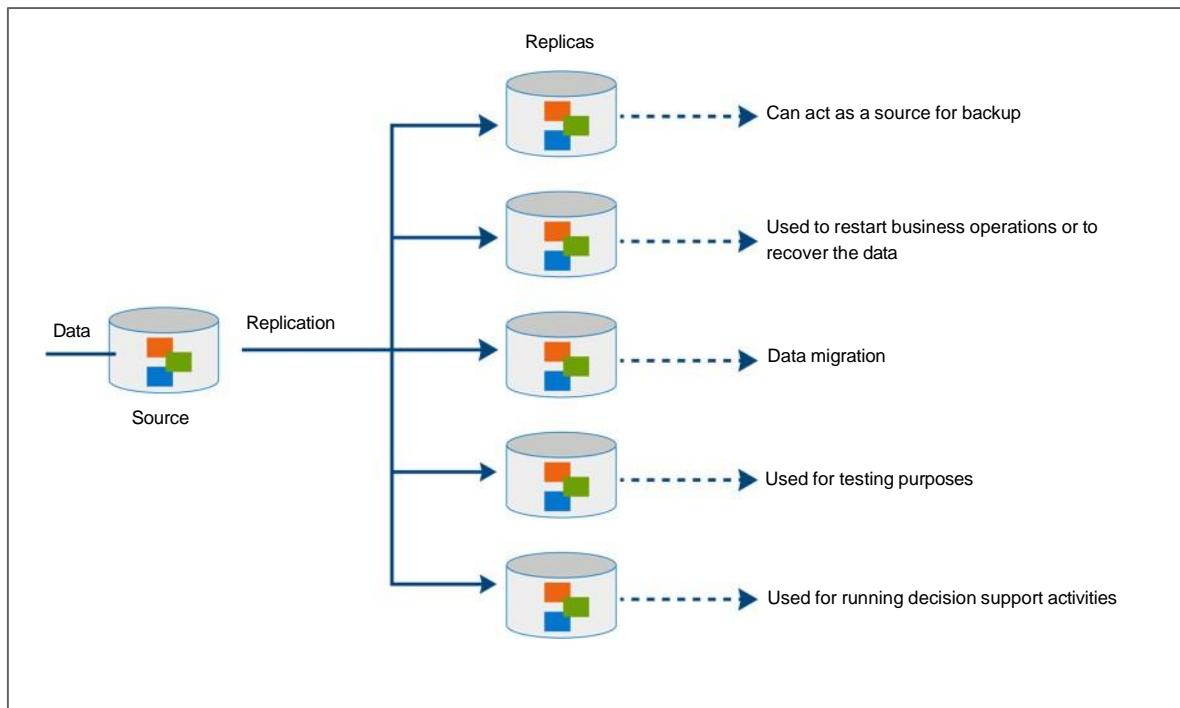
---

<sup>67</sup> In a replication environment, a compute system accesses the production data from one or more LUNs on a storage system. These LUNs are known as source LUNs, production LUNs, or the source. A LUN on which the production data is replicated to is called the target or replica.

## Data Replication

- For example, the production data is copied from the source (primary storage) to the target. The target can be other storage in the same data center, storage in a different data center, or to the cloud.

## Use of Replicas



### Notes:

**Alternative source for backup:** Under normal backup operations, data is read from the production LUNs and written to the backup device. This approach places an additional burden on the production infrastructure because production LUNs are simultaneously involved in production operations and servicing data for backup operations. To avoid this situation, a replica can be created from production LUN and it can be used as a source to perform backup operations. This method alleviates the backup I/O workload on the production LUNs.

**Fast recovery and restart:** For critical applications, replicas can be taken at short, regular intervals. This approach allows easy and fast recovery from data loss. If a complete failure of the source (production) LUN occurs, the replication solution enables one to restart the production operation on the replica to reduce the RTO.

**Decision-support activities**, such as reporting: Running reports using the data on the replicas greatly reduces the I/O burden that is placed on the production device.

## Data Replication

**Testing platform:** Replicas are also used for testing new applications or upgrades. For example, an organization may use the replica to test the production application upgrade; if the test is successful, the upgrade may be implemented on the production environment.

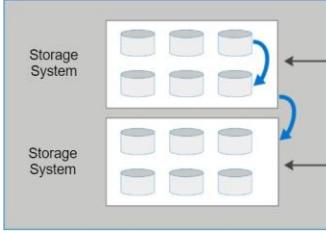
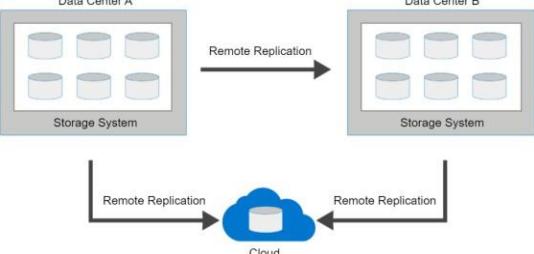
**Data migration:** Another use for a replica is data migration. Data migrations are performed for various reasons such as migrating from a smaller capacity LUN to one of a larger capacity for newer versions of the application.

## Data Replication: Additional Information



*To understand more about replication, click [here](#).*

### Types of Replication

Local Replication	Remote Replication
 <p><b>Local replication</b></p> <p>Data is replicated within a storage system in a storage-based replication</p> <p>Data is replicated within a data center from one system to another in a compute-based replication</p>	 <p><b>Remote replication</b></p>
<ul style="list-style-type: none"> <li>Replicating data within the same location.             <ul style="list-style-type: none"> <li>Within a data center.</li> <li>Within a storage system.</li> </ul> </li> <li>It is typically used for operational restore of data when there is data loss.</li> </ul>	<ul style="list-style-type: none"> <li>Replicating data to remote locations (locations can be geographically dispersed).             <ul style="list-style-type: none"> <li>Data can be synchronously or asynchronously replicated.</li> <li>It helps to mitigate the risks associated with regional outages.</li> </ul> </li> <li>It enables organizations to replicate the data to cloud for DR purpose.</li> </ul>

## Local Replication: Snapshot

A **snapshot** is a virtual copy of a set of files, VM, or LUN as they appeared at a specific point-in-time (PIT). A point-in-time copy of data contains a consistent image of the data as it appeared at a given point in time.

Snapshots can establish recovery points in a small fraction of time and can reduce Recovery Point Objective (RPO) by supporting more frequent recovery points. If a file is lost or corrupted, it can typically be restored from the latest snapshot data in a few seconds.

### VM Snapshot

- A VM snapshot preserves the state and data of a VM at a specific PIT, enabling quick restoration of a VM.
  - The snapshot includes the power state of a VM (powered-on, powered-off, or suspended).
  - The data includes all the files that make up the VM.
- For example:
  - Administrator can create a snapshot of a VM, make changes such as applying patches and software upgrades to the VM.
  - If anything goes wrong, the administrator can restore the VM to its previous state using the VM snapshot.
- Taking multiple snapshots provide several restore points for a VM.

### Storage System-Based Snapshot

- Storage system-based snapshot provides space optimal pointer-based virtual replication.
- At the time of replication session activation, the target (snapshot) contains pointers to the location of the data on the source.
- The snapshot does not contain data at any time. The snapshot is known as a virtual replica.

## Data Replication

- The snapshot is immediately accessible after the replication session activation.

### Notes:

Multiple snapshots can be created from the same source LUN for various business requirements. Some snapshot software provides the capability of automatic termination of a snapshot upon reaching the expiration date. The unavailability of the source device invalidates the data on the target. The storage system-based snapshot uses a Redirect on Write (RoW) mechanism.

RoW redirects new writes that are destined for the source LUN to a reserved LUN in the storage pool. In RoW, a new write from source compute system is written to a new location (redirected) inside the pool. The original data remains where it is, and is therefore read from the original location on the source LUN and is untouched by the RoW process.

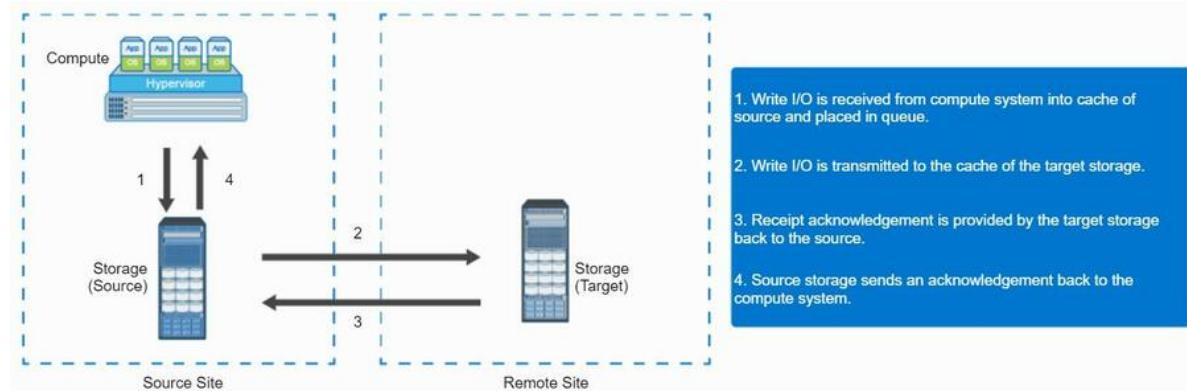
## Local Replication: Clone

- Cloning provides the ability to create fully populated point-in-time copies of LUNs within a storage system or create a copy of an existing VM.
- **Clone of a storage volume**
  - Initial synchronization is performed between the source LUN and the replica (clone).
  - During the synchronization process, the replica is not available for any compute system access. Once the synchronization is completed, the replica is exactly same as the source LUN.
  - Data changes made to both the source and the replica can be tracked at some predefined granularity.
- **VM clone**
  - Clone is a copy of an existing virtual machine (parent VM).
  - Typically clones are deployed when many identical VMs are required that reduces the time that is required to deploy a new VM.
  - Two types of clones:

<b>Full clone</b>	It is an independent copy of a VM that shares nothing with the parent VM.
<b>Linked clone</b>	It is created from a snapshot of the parent VM.

### Remote Replication: Synchronous

- Write is committed to both the source and the remote replica before it is acknowledged to the compute system.
- Synchronous replication enables restarting business operations at a remote site with zero data loss and provides near zero RPO.



**Synchronous remote replication process**

#### Notes:

Storage-based remote replication solution can avoid downtime by enabling business operations at remote sites. Storage-based synchronous remote replication provides near zero RPO where the target is identical to the source always.

In synchronous replication, writes must be committed to the source and the remote target prior to acknowledging “write complete” to the production compute system. Another writes on the source cannot occur until each preceding write has been completed and acknowledged.

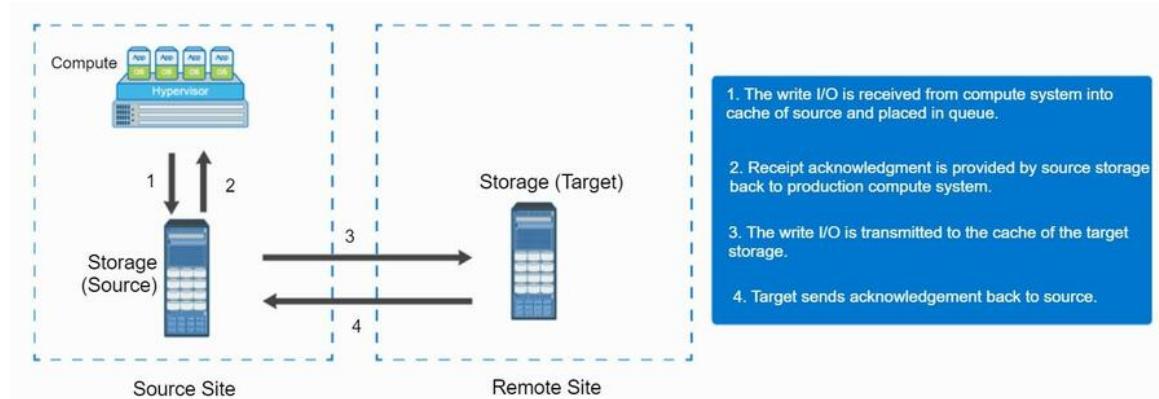
This approach ensures that data is identical on the source and the target always. Further, writes are transmitted to the remote site exactly in the order in which they are received at the source. Write ordering is maintained and it ensures transactional consistency when the applications are restarted at the remote location. As a result, the remote images are always restartable copies.

Application response time is increased with synchronous remote replication. Since, writes must be committed on both the source and the target before sending the “write complete” acknowledgment to the compute system. The degree of impact on

response time depends primarily on the distance and the network bandwidth between sites. If the bandwidth provided for synchronous remote replication is less than the maximum write workload, there are times during the day when the response time might be excessively elongated, causing applications to time out. The distances over which synchronous replication can be deployed depend on the capability of an application to tolerate the extensions in response time. Typically, synchronous remote replication is deployed for distances less than 200 kilometers (125 miles) between the two sites.

### Remote Replication: Asynchronous

- A write is committed to the source and immediately acknowledged to the compute system.
- Data is buffered at the source and sent to the remote site periodically.
- Replica is behind the source by a finite amount (finite RPO).



***Asynchronous remote replication process***

#### Notes:

It is important for an organization to replicate data across geographical locations to mitigate the risk involved during disaster. If the data is replicated (synchronously) between sites and the disaster strikes, then there would be a chance that both the sites may be impacted. This method may lead to data loss and service outage.

Asynchronous replication enables to replicate data across sites which are 1000s of kilometers apart.

In asynchronous remote replication, a write from a production compute system is committed to the source and immediately acknowledged to the compute system. Asynchronous replication also mitigates the impact to the response time of an application because the writes are acknowledged immediately to the compute system.

In asynchronous replication, compute system writes are collected into buffer (delta set) at the source. This delta set is transferred to the remote site in regular

intervals. Adequate buffer capacity should be provisioned to perform asynchronous replication. Some storage vendors offer a feature called delta set extension, which enables to offload delta set from buffer (cache) to specially configured drives. This feature makes asynchronous replication resilient to the temporary increase in write workload or loss of network link.

In asynchronous replication, RPO depends on the size of the buffer, the available network bandwidth, and the write workload to the source. This replication can take advantage of locality of reference (repeated writes to the same location). If the same location is written multiple times in the buffer prior to transmission to the remote site, only the final version of the data is transmitted. This feature conserves link bandwidth.

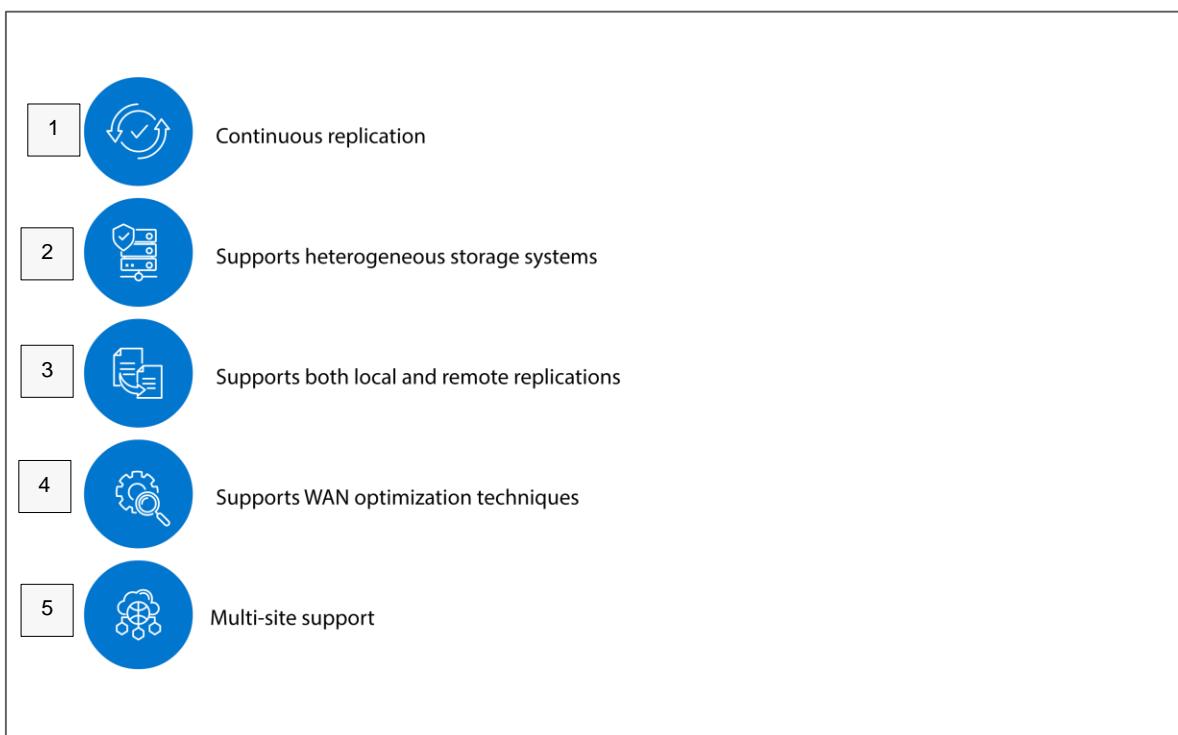
## Replication Types: Additional Information



*To understand more about various types of replication, click [here](#).*

## Continuous Data Protection (CDP)

- Continuous Data Protection provides the capability to restore data and VMs to any previous point-in-time (PIT).
  - Data changes are continuously captured and stored at a separate location from the production volume so that the data can be restored to any previous PIT.



**1:** Continuous Data Protection provides continuous replication, tracks all the changes to the production volumes that enable to recover to any point-in-time.

**2:** Continuous Data Protection solutions have the capability to replicate data across heterogeneous storage systems.

**3:** Continuous Data Protection supports both local and remote replication of data and VMs to meet operational and disaster recovery respectively.

**4:** Continuous Data Protection supports various WAN optimization techniques (deduplication, compression, and fast write) to reduce bandwidth requirements and also optimally uses the available bandwidth.

## Data Replication

**5:** Continuous Data Protection supports multisite replication, where the data can be replicated to more than two sites using synchronous and asynchronous replication.

## Key Continuous Data Protection Components

- Contains all the data that has changed from the time the replication session started

- Amount of space that is configured for the journal determines how far back the recovery points can go

Journal Volume

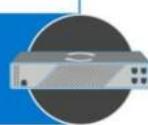


- Intelligent hardware platform that runs the CDP software

- Manages both the local and remote replications

- Appliance can also be virtual

CDP Appliance



- Intercepts writes to the production volume and splits each write into two copies

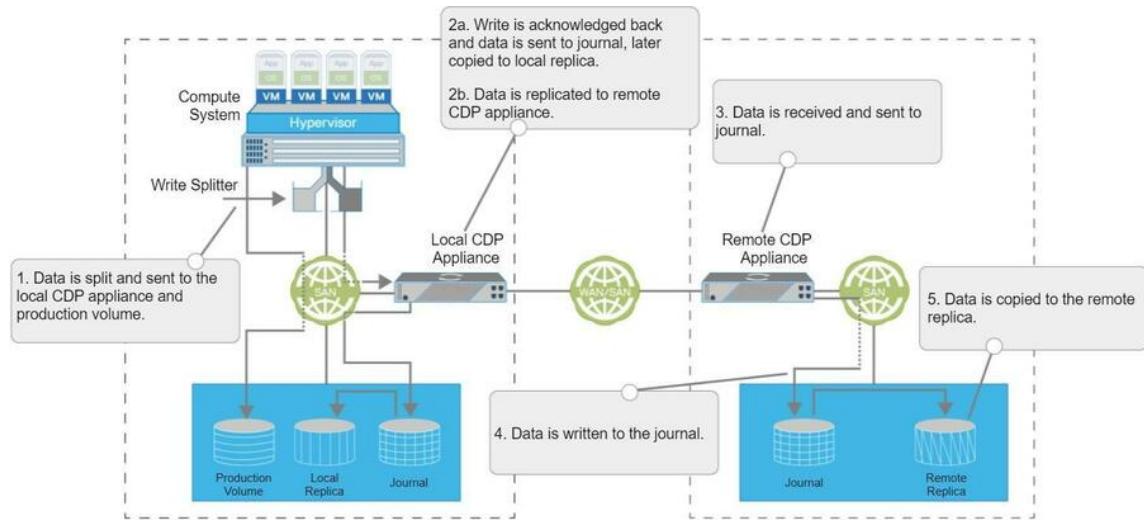
- Can be implemented at the compute, fabric, or storage system

Write Splitter



*Continuous Data Protection (CDP) components*

### Continuous Data Protection: Local and Remote Replication



#### Notes:

Typically, the replica is synchronized with the source, and then the replication process starts. After the replication starts, all the writes from the compute system to the source (production volume) are split into two copies. One copy is sent to the local Continuous Data Protection appliance at the source site, and the other copy is sent to the production volume. Then the local appliance writes the data to the journal at the source site and the data in turn is written to the local replica. If a file is accidentally deleted, or the file is corrupted, the local journal enables organizations to recover the application data to any PIT.

In remote replication, the local appliance at the source site sends the received write I/O to the appliance at the remote (DR) site. Then, the write is applied to the journal volume at the remote site. As a next step, data from the journal volume is sent to the remote replica at predefined intervals. Continuous Data Protection operates in either synchronous or asynchronous mode.

## CDP: Additional Information



*To understand about continuous data replication, click [here](#).*

Knowledge Check

## Knowledge Check

## Knowledge Check

1. Which provides the ability to create fully populated point-in-time copies of LUNs within a storage system or create a copy of an existing VM?
  - a. Clone
  - b. Snapshot
  - c. Pointer-based virtual replica
  - d. Full volume virtual replica

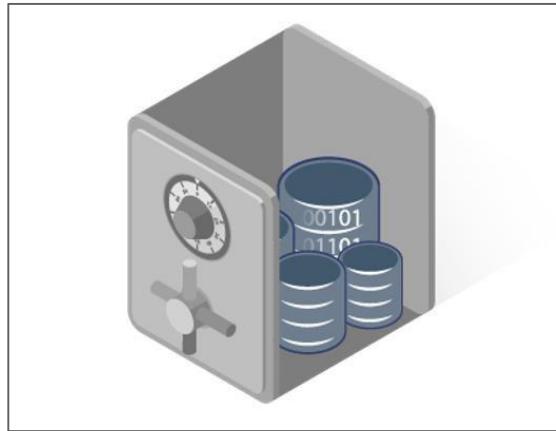
Data Backup

## Data Backup

## Data Backup

## Backup Overview

A Backup is an additional copy of production data, which is created and retained for the sole purpose of recovering lost or corrupted data.



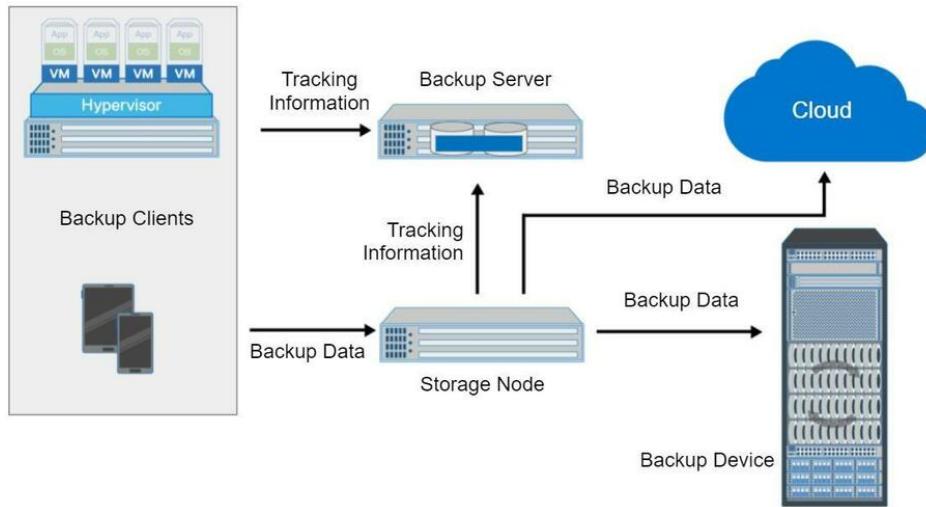
Organizations implement backups in order to protect the data from accidental deletion, application crashes, data corruption, and disaster.

An organization needs data backups to:

- Recover the lost or corrupted data for smooth functioning of business operations.
- Comply with regulatory requirements.
- Avoid financial and business loss.

## Backup Architecture

In a backup environment, the common backup components are **Backup Client**, **Backup Server**, **Storage Node**, and **Backup Target (Backup Device)**.



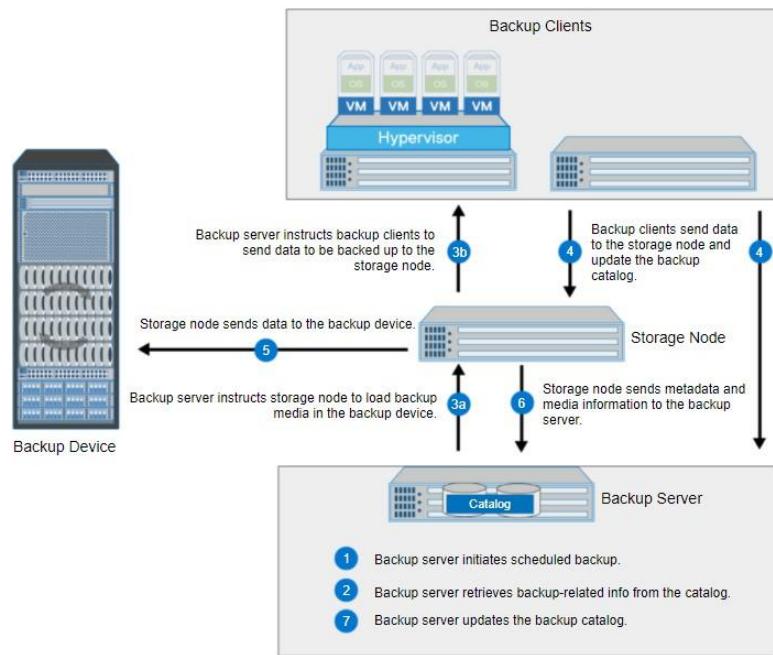
### Notes:

The role of a **backup client** is to gather the data that must be backed up and send it to the storage node. The backup client can be installed on application servers, mobile clients, and desktops. It also sends the tracking information to the backup server.

The **backup server** manages the backup operations and maintains the backup catalog, which contains information about the backup configuration and backup metadata. The backup configuration contains information about when to run backups, which client data to be backed up, and so on. The backup metadata contains information about the backed-up data. The **storage node** is responsible for organizing the client's data and writing the data to a backup device. A storage node controls one or more backup devices.

In most implementations, the storage node and the backup server run on the same system. Backup devices may be attached directly or through a network to the storage node. The storage node sends the tracking information about the data that is written to the backup device to the backup server. Typically this information is used for recoveries. Backup targets include tape, disk, virtual disk library, and the cloud.

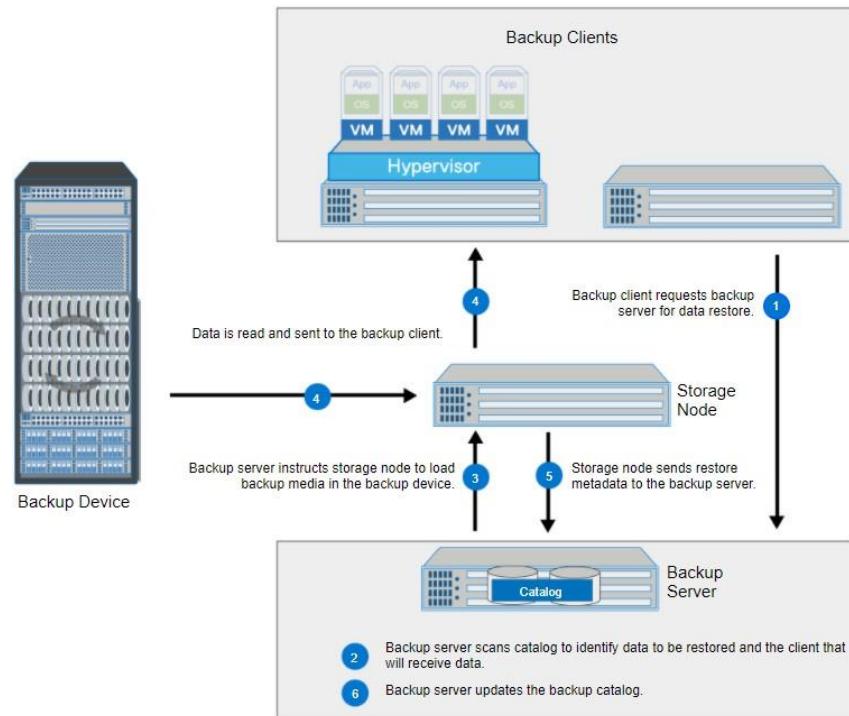
### Backup Operation



#### Steps to perform backup operation

## Recovery Operation

After the data is backed up, it can be restored when required. A recovery operation restores data to its original state at a specific Point in Time (PIT). Typically, backup applications support restoring one or more individual files, directories, or VMs.



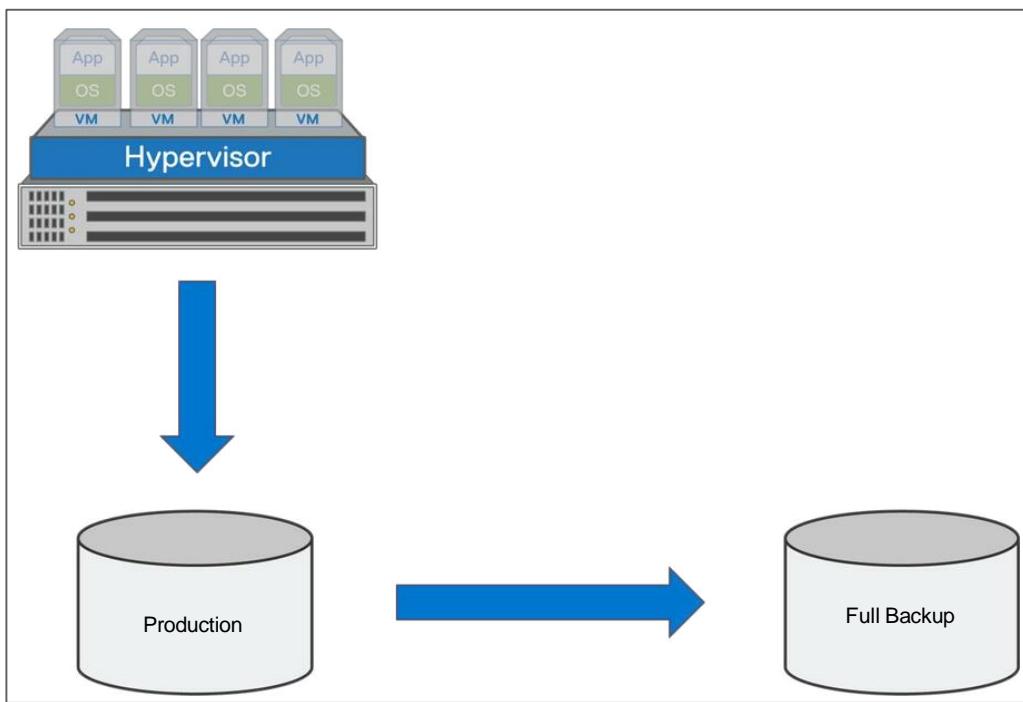
**Steps to perform recovery operation**

### Backup Granularities

Backups can be categorized as ***Full, Incremental, and Cumulative (or Differential)***.

#### Full Backup

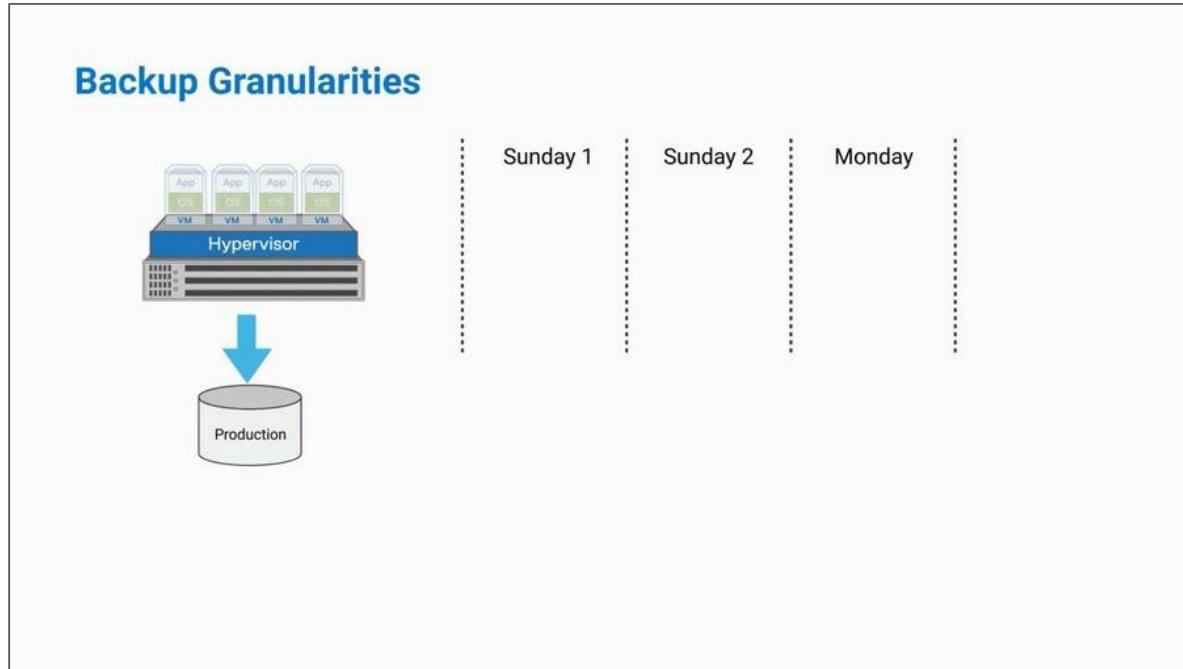
- Full backup copies all data on the production volume to a backup device.
  - It provides a faster data recovery.
  - It requires more storage space and takes more time to backup.



#### Full Backup-Restore

In the motion graphics shown below, a full backup is created on every Sunday. When there is a data loss in the production on Monday, the recent full backup that is created on the previous Sunday is used to restore the data in the production.

- Recovery Point Objective (RPO) determines which backup copy is used to restore the production.



## Incremental Backup

Incremental backup copies the data that has changed since the last backup.

- The main advantage of incremental backups is that fewer files are backed up daily, allowing for shorter backup windows<sup>68</sup>.
  - Click [here](#)<sup>69</sup> to view the example of incremental backup.
- 

<sup>68</sup> It is the period during which a production volume is available to perform a backup.

<sup>69</sup> For example, as shown in the motion graphic, a full backup is created on Sunday, and incremental backups are created for the rest of the week. Backup that is created on Monday would contain only the data that has changed since Sunday. Backup that is created on Tuesday would contain only the data that has changed since Monday. Backup that is created on Wednesday would only contain the data

## Data Backup



### Cumulative Backup

Cumulative (differential) backup copies the data that has changed since the last full backup.

- The advantage of differential backups over incremental backup is shorter restore times.

---

that has changed since Tuesday. The primary disadvantage to incremental backups is that they can be time-consuming to restore. Suppose that an administrator wants to restore the backup from Wednesday. The administrator has to first restore full backup that is created on Monday. After that, the administrator has to restore backup that is created on Tuesday, then followed by backup created on Wednesday.

- The tradeoff is that as time progresses, a differential backup can grow to contain more data than an incremental backup.
  - Click [here](#)<sup>70</sup> to view the example of cumulative backup.
- 

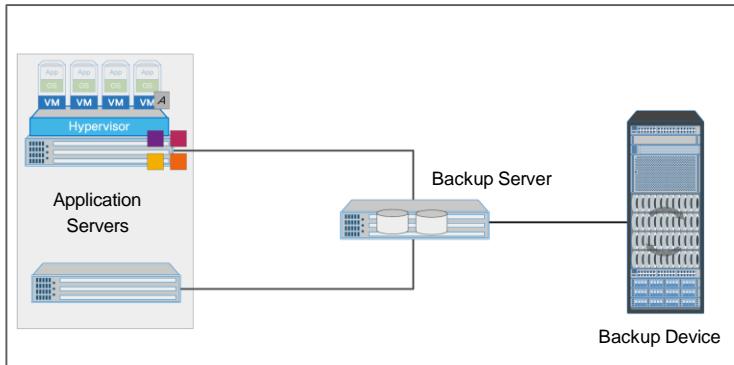
<sup>70</sup> For example, the administrator created a full backup on Sunday and differential backups for the rest of the week. Backup that is created on Monday would contain all the data that has changed since Sunday. It would therefore be identical to an incremental backup at this point. On Tuesday, however, the differential backup would backup any data that had changed since Sunday (full backup). The advantage that differential backups have over incremental is shorter restore times. Restoring a differential backup never requires more than two copies. The tradeoff is that as time progresses, a differential backup can grow to contain more data than an incremental backup. Suppose that an administrator wants to restore the backup from Tuesday. The administrator has to first restore the full backup that is created on Sunday. After that, the administrator has to restore the backup created on Tuesday.

## Data Backup



## Agent-Based Backup

In this approach, an agent or client is installed on a virtual machine (VM) or a physical compute system. The agent streams the backup data to the backup device.



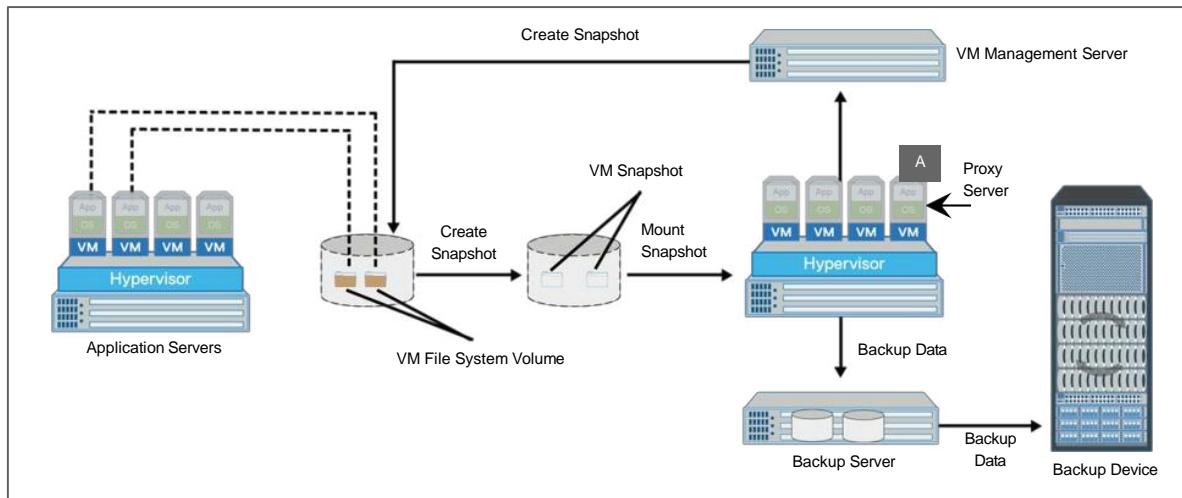
***Agent-based backup***

- Agent-based backup supports file-level backup and restore.
  - It impacts performance of applications running on compute systems.
  - The agent running on the compute system consumes CPU cycles and memory resources.

## Data Backup

### Image-Based Backup

Image-based backup makes a copy of the virtual machine disk and configuration that is associated with a particular VM. The backup is saved as a single entity called a VM image.



***Image-based backup process***

- In an image-based backup, the backup software can:
  - Send request to the VM management server to create a snapshot of the VMs to be backed up and mount it on the proxy server.
- Backup is performed using the snapshot by the proxy server.

#### Notes:

This backup is used for restoring an entire VM if there is any hardware failure or human error. It is also possible to restore individual files and folders within a virtual machine.

In an image-level backup, the backup software can backup VMs without installing backup agents inside the VMs or at the hypervisor-level. Proxy server performs the backup operations, and it acts as the backup client. The proxy server offloads the backup processing from the VMs.

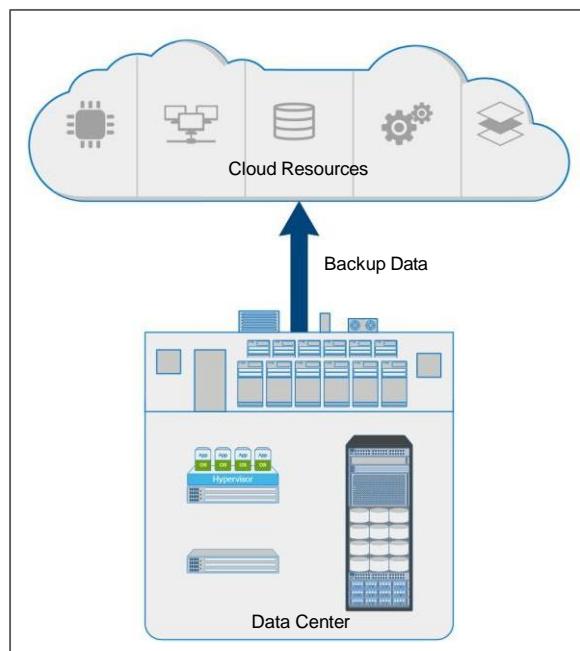
The proxy server communicates to the management server responsible for managing the virtualized compute environment. It sends commands to create a snapshot of the VM to be backed up and to mount the snapshot to the proxy

server. A snapshot captures the configuration and virtual disk data of the target VM and provides a point-in-time view of the VM.

The proxy server then performs backup by using the snapshot. Performing an image-level backup of a virtual machine disk enables running a bare metal restore of a VM.

Some of the vendors support changed block tracking mechanism. This feature identifies and tags any blocks that have changed since the last VM snapshot. This method enables the backup application to backup only the blocks that have changed, rather than backing up every block.

### Cloud-Based Backup (Backup as a Service)



Organizations must regularly protect the data to avoid losses, stay compliant, and preserve data integrity. They may face challenges on IT budget, and IT management. These challenges can be addressed with the emergence of cloud-based data protection.

- It enables consumers to procure backup services on-demand.
- It reduces the backup management overhead.
- Cloud-based backup gives the consumers the flexibility to select a backup technology based on their current requirements.

## Backup Architecture: Additional Information



*To understand more about backup architecture, click [here](#).*

## Backup and Recovery Lab Demo



To view the demo of performing backup and recovery using Dell EMC NetWorker, click [here](#).

## Knowledge Check

## Knowledge Check

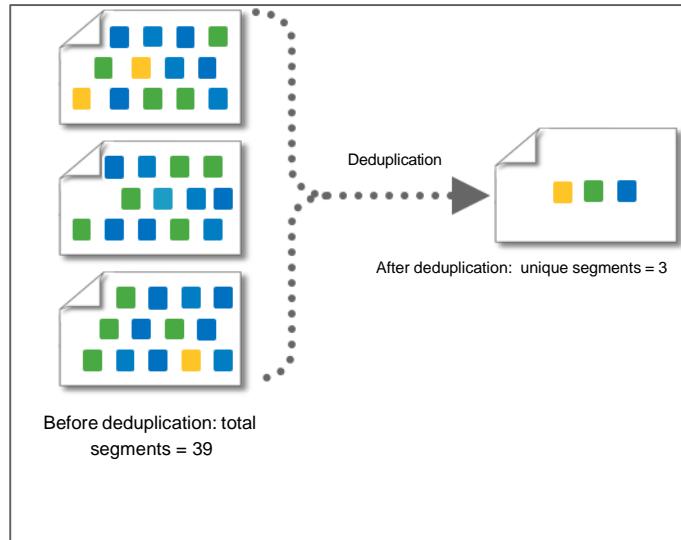
### Knowledge Check

1. Which backup component manages the backup operations and maintains the backup catalog?
  - a. Backup client
  - b. Backup target
  - c. Backup server
  - d. Backup device

## Data Deduplication

### Data Deduplication Overview

**Challenges of duplicate data in a data center:**



*Example of data deduplication.*

- Difficult to protect the data within the budget.
- Duplicate data impacts the backup window.
- It increases network bandwidth.

Data deduplication provides a solution for organizations to overcome these challenges in a backup and production environment.

**Data Deduplication** is the process of detecting and identifying the unique data segments within a given set of data to eliminate redundancy.

- Effectiveness of deduplication is expressed as a deduplication ratio<sup>71</sup>.

**Notes:**

In a data center environment, a certain percentage of data, which is retained on a backup media is redundant. The typical backup process for most organizations consists of a series of daily incremental backups and weekly full backups. Daily backups are retained for a few weeks and weekly full backups are retained for several months. Because of this process, multiple copies of identical or slowly changing data are retained on backup media, leading to a high level of data redundancy.

Many files are common across multiple systems in a data center environment. Many users across an environment store identical file such as Word documents, Microsoft PowerPoint presentations, and Excel spreadsheets. Backups of these systems contain many identical files. Also, many users keep multiple versions of files that they are working on. Many of these files differ only slightly from other versions, but are seen by backup applications as new data that must be protected.

Due to this redundant data, the organizations are facing many challenges. Backing up redundant data increases the amount of storage that is required to protect the data and then increases the storage infrastructure cost. It is important for organizations to protect the data within the limited budget. Organizations are running out of backup window time and facing difficulties meeting recovery

---

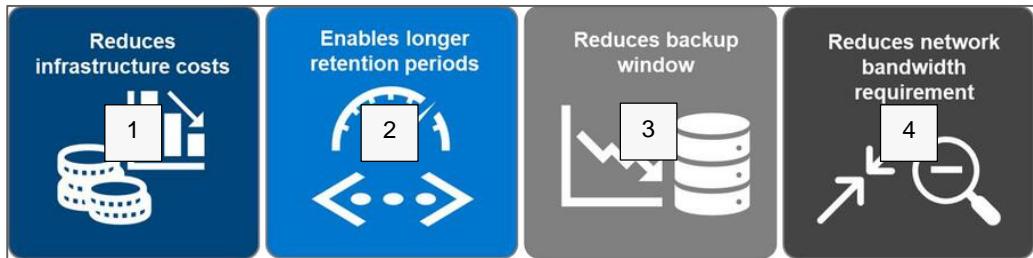
<sup>71</sup> It is the ratio of data before deduplication to the amount of data after deduplication. This ratio is typically depicted as “ratio:1” or “ratio X” (10:1 or 10 X). For example, if 200 GB of data consumes 20 GB of storage capacity after data deduplication, the space reduction ratio is 10:1.

## Data Deduplication

objectives. Backing up large amount of duplicate data at the remote site or cloud for DR purpose is also cumbersome and requires huge bandwidth.

Data deduplication provides a solution for organizations to overcome these challenges in a backup and production environment. Deduplication is the process of detecting and identifying the unique data segments (chunk) within a given set of data to eliminate redundancy. Only one copy of the data is stored; the subsequent copies are replaced with a pointer to the original data.

## Key Benefits of Data Deduplication



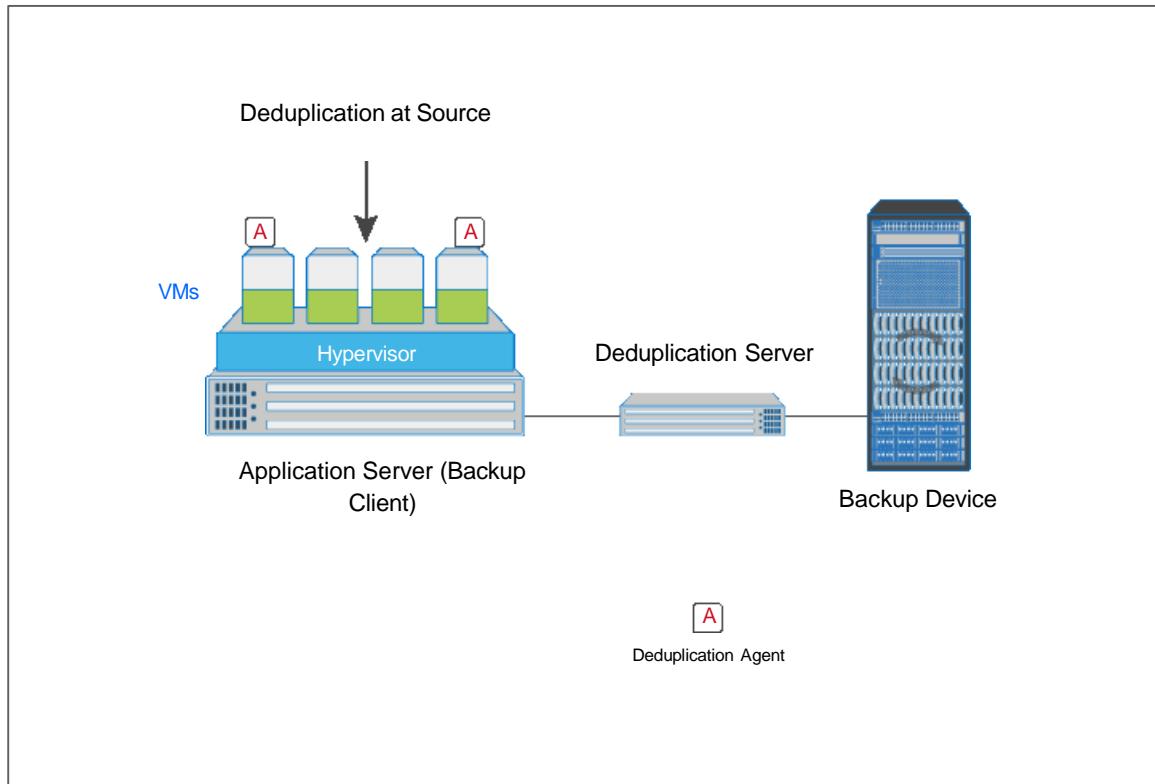
**1:** By eliminating redundant data from the backup, the infrastructure requirement is minimized. Data deduplication directly results in reduced storage requirements. Smaller storage needs result in lower acquisition costs as well as reduced power and cooling costs.

**2:** As data deduplication reduces the amount of content in the daily backup, users can extend their retention policies. This approach can have a significant benefit to users who require longer retention.

**3:** Data deduplication eliminates redundant content of backup data, which results in backing up less data and reduced backup window.

**4:** By using data deduplication at the client, redundant data is removed before the data is transferred over the network. This approach reduces the network bandwidth that is required for sending backup data to remote site for DR purpose.

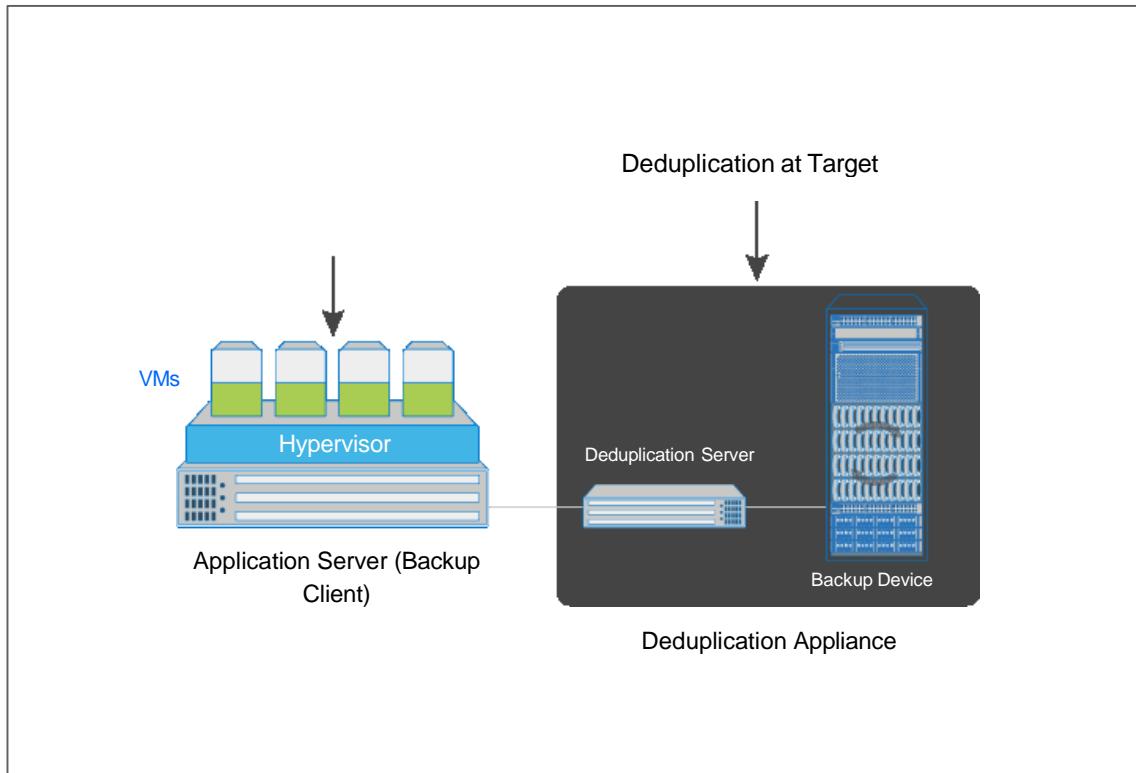
### Data Deduplication Method: Source-Based



#### ***Source-based data deduplication***

- Data is deduplicated at the source (backup client).
  - Backup client sends only new, unique segments across the network.
  - It reduces storage capacity and network bandwidth requirements.
  - It is recommended for Remote Office Branch Office (ROBO) environments for taking centralized backup.
- Cloud service providers use source-based method when performing backup from consumer's location to their location.

## Data Deduplication Method: Target-Based



### ***Target-based data deduplication***

- Data is deduplicated at the target.
  - Inline
  - Postprocess
- It offloads the backup client from the deduplication process.
- It requires sufficient network bandwidth.
- In some implementations, part of the deduplication load is moved to the backup server.
  - Reduces the burden on the target.
  - Improves the overall backup performance.

## Data Deduplication: Additional Information



*To understand about data deduplication, click [here](#).*

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. What is the benefit of implementing source-based deduplication?
  - a. Reduces the amount of data sent over the network.
  - b. Improves the performance of an application server (client)
  - c. Improves the performance of a backup device
  - d. Reduces the storage required to copy backup catalog

# Data Archiving

### Data Archiving Overview



Data archiving moves fixed content that is no longer actively accessed to a separate low-cost archive storage system for long-term retention and future reference.

- Data archiving saves primary storage capacity.
- Data archiving reduces backup window and backup storage cost.

#### Notes:

Data in the primary storage is actively accessed and changed. As data ages, it is less likely to change and eventually becomes “fixed” but continues to be accessed by applications and users. This data is called fixed data. Fixed data is growing at over 90 percent annually. Keeping the fixed data in primary storage systems poses several challenges.

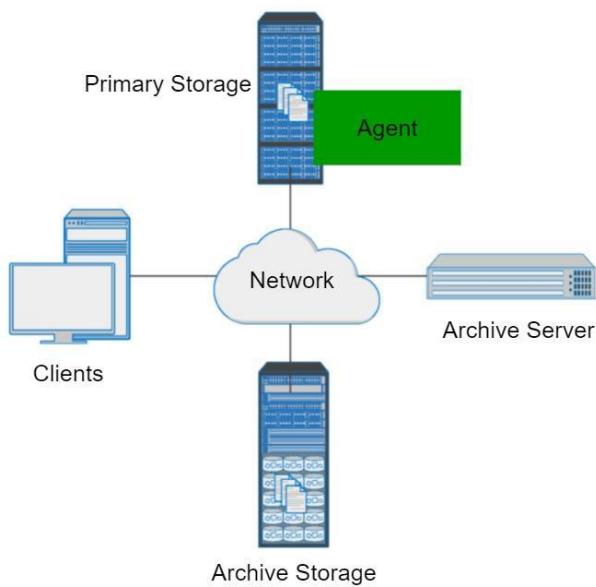
First, preserving data on the primary storage system causes increasing consumption of expensive primary storage. Second, data that must be preserved over a long period for compliance reasons may be modified or deleted by the users. These pose a risk of a compliance breach. Finally, the backup of high-growth fixed data results in an increased backup window and related backup storage cost. Data archiving addresses these challenges.

Data archiving is the process of moving fixed data that is no longer actively accessed to a separate lower-cost archive storage system for long-term retention and future reference. With archiving, the capacity on expensive primary storage can be reclaimed by moving infrequently accessed data to lower-cost archive storage.

## Backup vs. Archive

Data Backup	Data Archive
Secondary copy of data	Primary copy of data
Used for data recovery operations	Available for data retrieval
Primary objective – operational recovery and disaster recovery	Primary objective – compliance adherence and lower cost
Typically short-term (weeks or months) retention	Long-term (months, years, or decades) retention

### Data Archiving Operations



*Data archiving components and operations*

- The data archiving operation involves the archiving agent, the archive server (policy engine), and the archive storage.
- Archiving agent scans primary storage to find files that meet the archiving policy.
  - The archive server indexes the files.
- Once the files have been indexed, they are moved to archive storage and small stub<sup>72</sup> files are left on the primary storage.

---

<sup>72</sup> The stub file contains the address of the archived file. As the size of the stub file is small, it saves space on primary storage.

## Use Case: Email Archiving



- Email archiving is the process of archiving email messages from the mail server to an archive storage.
  - After the email is archived, it is retained for years, based on the retention policy.

### Legal Dispute

- Email archiving helps an organization to address legal disputes.
  - For example, an organization may be involved in a legal dispute. They must produce all email messages within a specified time period containing specific keywords that were sent to or from certain people.

### Government Compliance

- Email archiving helps to meet government compliance requirements such as Sarbanes-Oxley and SEC regulations.
  - For example, an organization must produce all email messages from all individuals that are involved in stock sales or transfers. Failure to comply with these requirements could cause an organization to incur penalties.

### Mailbox Space Savings

- Email archiving provides more mailbox space by moving old email messages to archive storage.

## Data Archiving

- For example, an organization may configure a quota on each mailbox to limit its size. A fixed quota for a mailbox forces users to delete email messages as they approach the quota size. However, users often must access email messages that are weeks, months, or even years old. With email archiving, organizations can free up space in user mailboxes and still provide user access to older email messages.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Which archiving component scans primary storage to find files that meet the archiving policy?
  - a. Archiving agent
  - b. Archiving storage
  - c. Archiving client
  - d. Archiving policy engine

## Data Migration

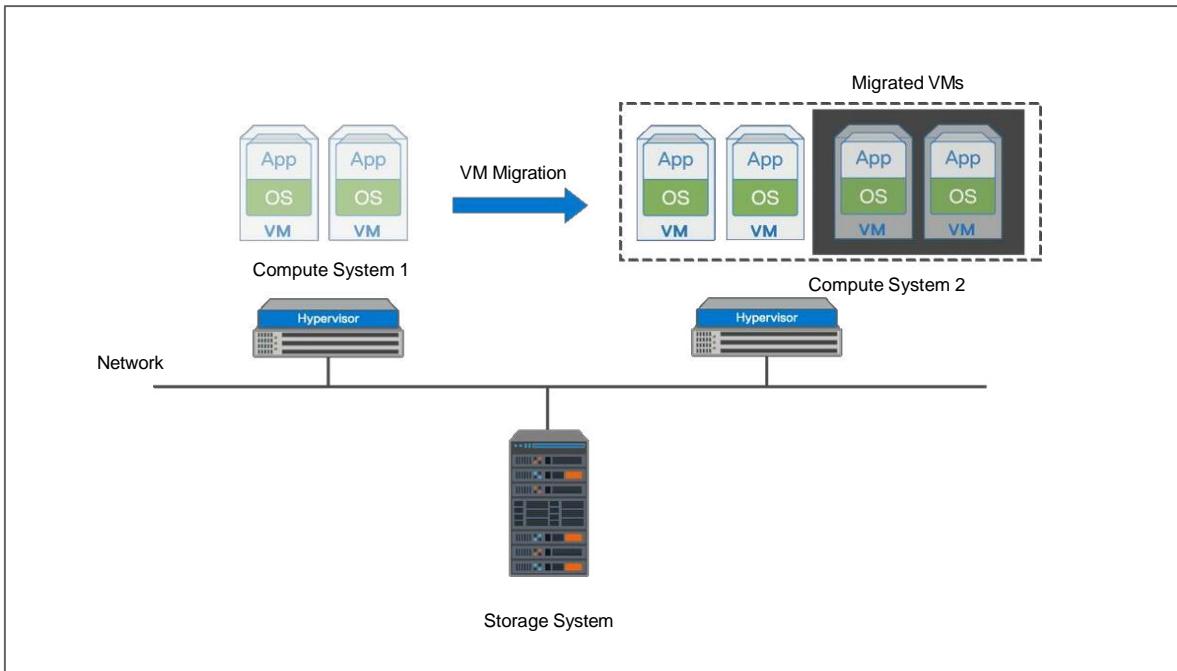
## Data Migration Overview

**Data migration** is a specialized replication technique that enables moving data from one system to another within a data center, between data centers, between cloud, and between data center and cloud. It transfers the data between hosts (physical or virtual), storage devices, or formats.

- In today's competitive business environment, IT organizations should require nondisruptive live migration solutions in place to meet the required SLAs.
- Organization deploys data migration solutions for the following reasons:
  - Data center maintenance without downtime.
  - Avoid production impacts due to natural disasters.
  - Facilitate technology upgrades and refreshes.
  - Data center migration or consolidation.
  - Workload balancing across data centers.

## Hypervisor-Based Migration

### VM Migrations



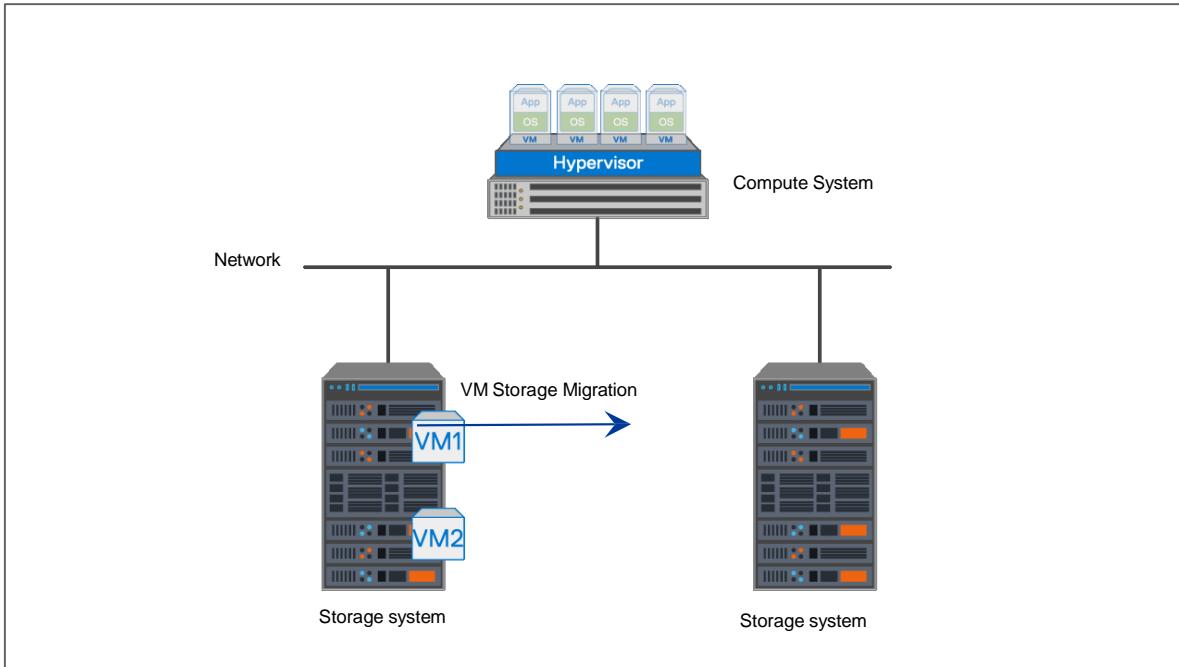
#### ***VM migration between compute systems***

In this type of migration, virtual machines (VMs) are moved from one physical compute system to another without any downtime. VM migration method enables:

- Scheduled maintenance without any downtime.
- VM load balancing.

## Data Migration

### VM Storage Migration



#### ***VM storage migration between storage systems***

In a VM storage migration, VM files are moved from one storage system to another system without any downtime or service disruption.

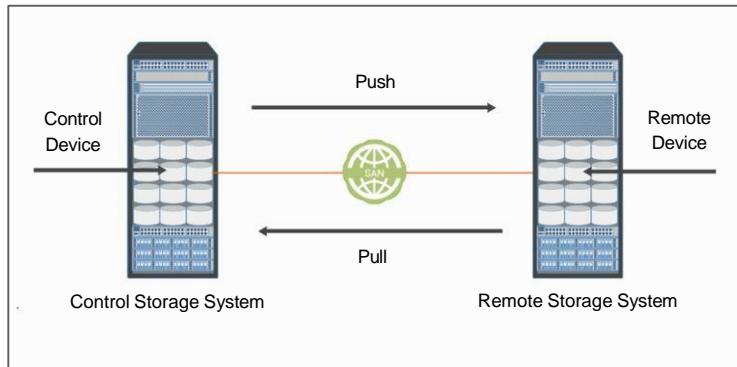
Key benefits of this type of migration are as follows:

- It simplifies array migration and storage upgrades.
- Dynamically optimizes storage I/O performance.
- Efficiently manages storage capacity.

## Storage-Based Data Migration

Storage-based migration moves block-level and file-level data between heterogeneous storage systems.

### SAN-based Migration



***SAN-based migration***

- SAN-based migration moves block-level data between heterogeneous storage systems over SAN.
- Storage system that performs migration is called the control storage system.
- Data migration solutions perform push<sup>73</sup> and pull<sup>74</sup> operations for data movement.

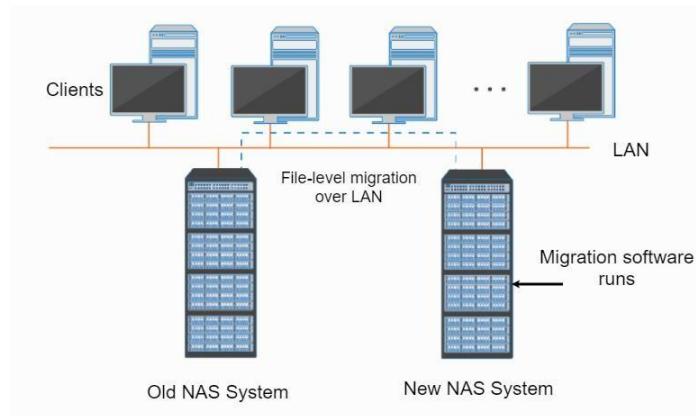
---

<sup>73</sup> Data is pushed from control system to remote system.

<sup>74</sup> Data is pulled from the remote system to control system.

## Data Migration

### NAS-based Migration



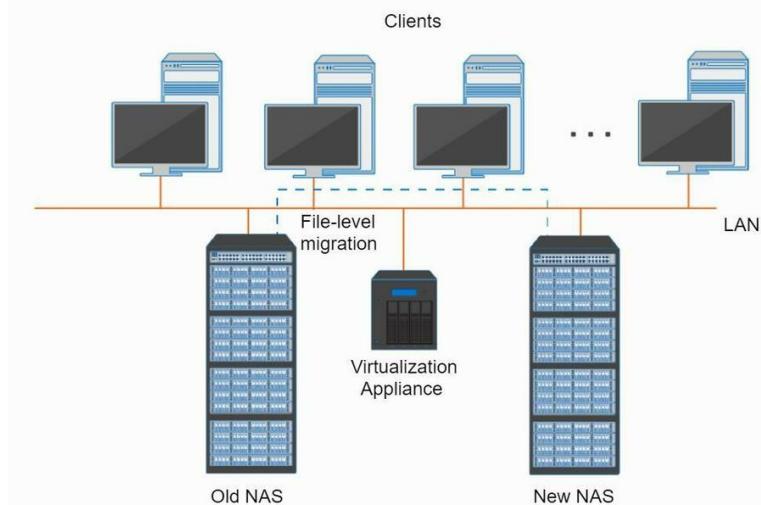
#### ***NAS-based migration***

- NAS-based migration moves file-level data between NAS systems over LAN or WAN.

In this example, the new NAS system initiates the migration operation and pulls the data directly from the old NAS system over the LAN. The key advantage of NAS to NAS direct data migration is that there is no need for an external component (host or appliance) to perform or initiate the migration process.

## Appliance-Based Data Migration

- Virtualization appliance facilitates the movement of files from an old NAS system to a new NAS system.



- While the files are being moved, clients can access their files nondisruptively.
  - Clients can also read their files from the old location and write them back to the new location without realizing that the physical location has changed.
- Virtualization appliance creates a virtualization layer that eliminates the dependencies between the data that is accessed at the file level and the location where the files are physically stored.

## VM Migration: Additional Information



*To understand about virtual machine migration, click [here](#).*

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Which migration moves file-level data between file servers over LAN or WAN?
  - a. NAS-based
  - b. Byte-based
  - c. SAN-based
  - d. Block-based

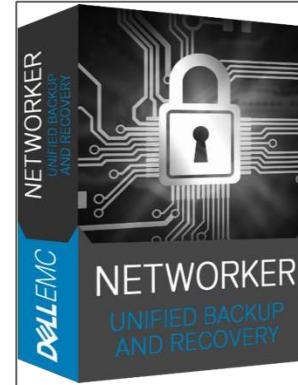
## Concepts in Practice

## Concepts in Practice

### Dell EMC NetWorker

Dell EMC NetWorker is a backup and recovery solution for mission-critical business applications in physical and virtual environments for on-premises and cloud.

- Unified backup and recovery software for the enterprise: Deduplication, backup to disk and tape, snapshots, replication and NAS.
- NetWorker provides a robust cloud capability enabling long-term retention to the cloud, backup to the cloud and backup in the cloud.
- NetWorker Module for Databases and Applications (NMDA) provides a data protection solution for DB2, Informix, MySQL, Oracle, SAP IQ, and Sybase ASE data.



### Dell EMC PowerProtect Data Manager



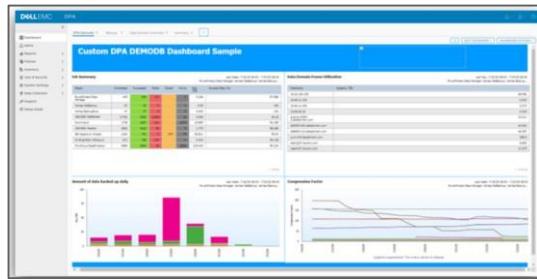
Dell EMC PowerProtect Data Manager provides software defined data protection, automated discovery, deduplication, operational agility, self-service and IT governance for physical, virtual and cloud environments.

#### PowerProtect Data Manager:

- Enables the protection, management, and recovery of data in on-premises, virtualized, and cloud deployments, including protection of in-cloud workloads.

- Enables the protection of traditional workloads including Oracle, Exchange, SQL, and file systems as well as Kubernetes containers and virtual environments.
- Restores data on-premises or in the cloud. Governance control ensures IT compliance, making even the strictest service level objectives obtainable.

## Dell EMC Data Protection Advisor (DPA)



DPA is a reporting and analytics platform that provides full visibility into the effectiveness of your data protection strategy. It can automate and centralize the collection and analysis of all data.

### Dell EMC Data Protection Advisor:

- Provides visibility across physical and virtual environments from a unified dashboard.
- Provides real-time monitoring and alerting of protection software and storage.
- Allows automated discovery of data protection infrastructure.

## Dell EMC PowerProtect DP Series Appliance

PowerProtect DP series appliances deliver powerful backup and recovery of all organization's data, wherever it lives, using a single appliance.



- PowerProtect Appliance is the next generation of Integrated Data Protection Appliance (IDPA). It is all-in-one data protection software and storage in a single appliance that delivers backup, replication, recovery, search, analytics and more.

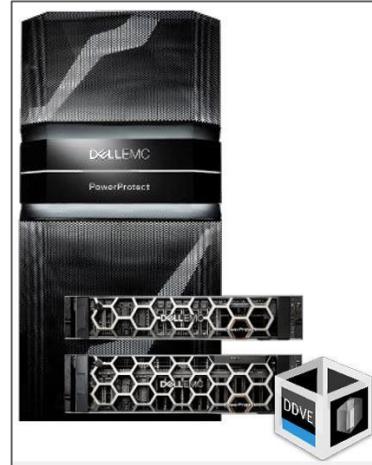
## Concepts in Practice

- Features include:
  - Systems can scale to Petabyte of usable capacity.
  - Cloud long-term retention and cloud DR-ready.
  - Provides VMware integration.
- PowerProtect Appliance supports native Cloud DR with end-to-end orchestration.
  - Allows enterprises to copy backed-up VMs from on-premises IDPA environments to a public cloud.

## Dell EMC PowerProtect DD Series Appliances

DD series enables organizations to protect, manage, and recover data at scale across their diverse environments.

- Integrates easily with existing infrastructures, enabling ease-of-use with leading backup and archiving applications.
- Natively tiers deduplicated data to any supported cloud environment for long-term retention with Dell EMC Cloud Tier.
- Provides fast disaster recovery with orchestrated DR and provides an efficient architecture to extend on-premises data protection.



PowerProtect DD Virtual Edition (DDVE) leverages the power of DDOS to deliver software-defined protection storage on-premises and in-cloud.

## Dell EMC TimeFinder SnapVX

TimeFinder SnapVX is a local replication solution for PowerMax, VMAX All Flash storage systems with cloud scalable snaps and clones to protect data. SnapVX solution:

- Provides space-efficient local snapshots that can be used for localized protection and recovery and other use cases including development, test, analytics, backups, and updating.
- Secures snapshots to prevent accidental or malicious deletion, securing them for a specified retention period.
  - The snapshots are made as efficient as possible by sharing point-in-time tracks which are called snapshot deltas.



## Dell EMC SRDF

SRDF is Dell EMC's remote replication technology for PowerMax. SRDF:

- Provides disaster recovery and data mobility solutions.
- Copies data between the sites independently without the host.
  - There are no limits to the distance between the source and the target copies.
- Enables storage systems to be in the same room, different buildings, or hundreds to thousands of kilometers apart.
- Provides the ability to maintain multiple, host-independent, remotely mirrored copies of data.

## Dell EMC RecoverPoint

Dell EMC RecoverPoint provides continuous data protection for comprehensive operational and disaster recovery.

- RecoverPoint for Virtual Machines is a hypervisor-based, software-only data protection solution for Virtual Machines.
- RecoverPoint:
  - Enables Continuous Data Protection for any point in time (PIT) recovery to optimize RPO and RTO.
  - Provides synchronous (sync) or asynchronous (async) replication policies.

## Concepts in Practice

- Reduces WAN bandwidth consumption and uses available bandwidth optimally.

## VMware vSphere HA and FT

- VMware vSphere High Availability (HA) leverages multiple ESXi hosts that are configured as a cluster to provide rapid recovery from outages.
  - Provides high availability for applications running in virtual machines.
  - Protects against a server failure by restarting the virtual machines on other hosts within the cluster.
  - Protects against application failure by continuously monitoring a virtual machine and resetting it if a failure is detected.
- VMware vSphere Fault Tolerance (FT) provides a higher level of availability.
  - Enables users to protect any virtual machine from a host failure with no loss of data, transactions, or connections.
  - Provides continuous availability by ensuring that the states of the Primary and Secondary VMs are identical at any point in time.
  - If either the host running the Primary VM or the host running the Secondary VM fails, an immediate and transparent failover occurs.

## Dell EMC Cloud Tier

Dell EMC Cloud Tier provides a solution for long-term retention. Using advanced deduplication technology that reduces storage footprints, unique data is sent to the cloud and data lands on the cloud object storage already deduplicated. Cloud tiering:

- Provides a native cloud tiering with no external appliance, or cloud gateway required.
- Enables efficient transfer of data to and from the cloud, using less bandwidth (source-side deduplication).

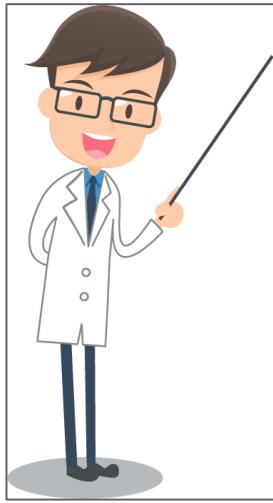
## Dell EMC Avamar

- Dell EMC Avamar enables fast, efficient backup and recovery through its integrated variable-length deduplication technology.

- Avamar is optimized for fast, daily full backups of physical and virtual environments, NAS servers, enterprise applications, remote offices and desktops/laptops.
- Dell EMC Avamar is proven backup and recovery software that delivers secure data protection for cloud, remote offices, desktops, laptops, and data centers.

## Exercise: Data Protection

## Exercise: Data Protection



### Scenario

A major multinational bank runs business-critical applications in a data center:

- They have multiple remote and branch offices (ROBO) across different geographic locations.
  - They use tape as the primary backup storage media for backing up virtual machines (VMs) and application data.
  - They use an agent-based backup solution for backing up data.
- The bank has a file-sharing environment in which multiple NAS systems serve all the users.
    - The data is backed up from application servers to backup device.
  - Approximately 25% of data in the production environment is inactive data (fixed content).
  - The bank has two data centers which are 1000 miles apart.

### Challenges

- Backup operations consume resources on the compute systems that are running multiple VMs.
  - This approach impacts the applications that are deployed on the VMs.
- Recovering data or VMs also takes more time.
- Backup environment has a huge amount of redundant data.
  - It increases the infrastructure cost and impacts the backup window.
- Branch offices also have limited IT resources for managing backup.

## Exercise: Data Protection

- Backing up data from branch offices to a centralized data center involve sending huge volumes of data over the WAN. It increases the cost of deployment.
- Organization incurs a huge investment and operational expense in managing an offsite backup infrastructure at remote site.

## Requirements

- Need faster backup and restore to meet the SLAs.
- Need to eliminate redundant copies of data.
- Need an effective solution to address the backup and recovery challenges of remote and branch offices.
- Need to offload the backup workload from the compute system to avoid performance impact to applications.
- The organization requires a strategy to eliminate backing up fixed content from the production environment.
- The organization requires a solution to reduce the management overhead and the investment cost in managing the offsite backup copy.
- The organization requires a remote replication solution for DR that should not impact the response time of the application.

## Deliverables

- Recommend solutions that meet the organization's requirements.

## Solutions

- Implement disk-based backup solution to improve the backup and recovery performance for meeting SLAs.
- Implement deduplication solution to eliminate the redundant copies of data.
- Organization can use disk-based backup solutions along with source-based deduplication.
  - Eliminate the challenges that are associated with centrally backing up remote office data.
  - Deduplication considerably reduces the required network bandwidth.

- Implement image-based backup that helps to offload backup operation from VMs to a proxy server.
  - No backup agent is required inside the VM to backup.
- Organization can implement data archiving solutions that archive fixed content from the production environment.
  - Reduce the amount of data to be backed up.
- Organization can choose backup as a service to replicate the offsite backup copy to the cloud.
  - It saves CAPEX and reduces the management overhead to the organization.
- To meet the DR requirement, the organization can implement asynchronous remote replication.
  - It provides finite RPO and does not impact response time.

# Storage Infrastructure Security

## Storage Infrastructure Security

## Introduction to Information Security

## Introduction to Information Security

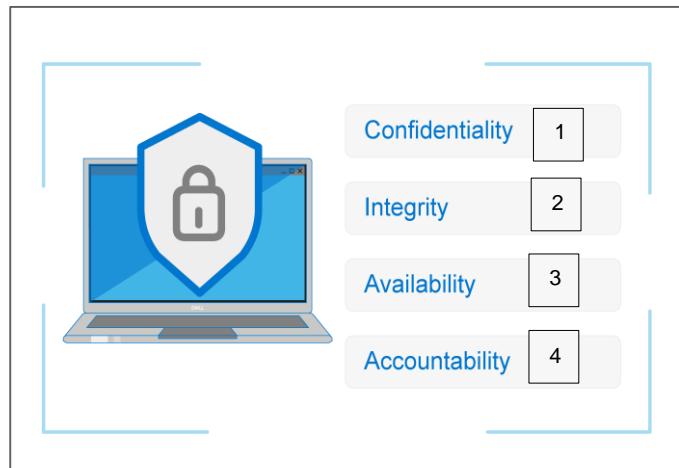


Information security includes a set of practices that protect data and information systems from unauthorized disclosure, access, use, destruction, deletion, modification, and disruption.

- Involves implementing various kinds of safeguards or controls in order to lessen the risk of an exploitation or a vulnerability in the information system.
- Deploys various tools to protect both data and infrastructure from unauthorized access, modification, and deletion.

## Information Security: Key Terminologies

The goals of information security are: Confidentiality, Integrity, Availability, and Accountability (CIAA).



**1:** Confidentiality provides the required secrecy of information to ensure that only authorized users have access to data.

**2:** Integrity ensures that unauthorized changes to information are not allowed. The objective of ensuring integrity is to detect and protect against unauthorized alteration or deletion of information.

**3:** Availability ensures that authorized users have reliable and timely access to compute, storage, network, application, and data resources.

**4:** Accountability is the process where the users or applications are responsible for the actions or events that are executed on the systems. Accountability can be achieved by auditing logs.

## Governance, Risk and Compliance (GRCA)

GRCA is a term encompassing processes that help an organization to ensure that their acts are ethically correct and in accordance with their:

- Risk appetite (the risk level an organization chooses to accept)
- Internal policies
- External regulations



**1:** Governance determines the purpose, strategy, and operational rules by which companies are directed and managed.

**2:** A systematic process of assessing its assets, placing a realistic valuation on each asset, and creating a risk profile that is rationalized for each information asset across the business.

**3:** An act of adhering to, and demonstrating adherence to external laws and regulations as well as to corporate policies and procedures.

### Notes:

To better understand GRC, consider an example of how GRC is implemented in an IT organization. In this example:

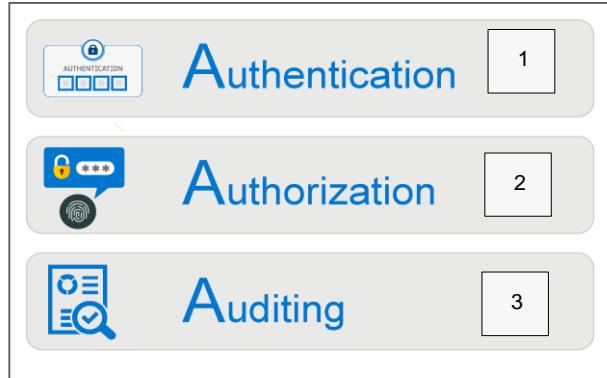
- A **Governance** group is the authority for making policies such as defining access rights to users based on their roles and privileges.

## Introduction to Information Security

- The **Risk management** team involves identifying resources that should not be accessed by certain users in order to preserve confidentiality, integrity, and availability.
- The **Compliance management** team assures that the policies are being enforced by implementing controls such as firewalls and identify management systems.

## Authentication, Authorization, and Auditing

For the GRC teams to achieve the desired CIAA goals, three key approaches are authentication, authorization, and auditing.



**1:**

- A process to ensure that users or assets are who they claim to be by verifying their identity credentials.
- A user may be authenticated by a single-factor<sup>75</sup> or multi-factor<sup>76</sup> method.

**2:**

- A process of determining whether and in which manner, a user, device, application, or process is allowed to access only the particular service or resource.

---

<sup>75</sup> Involves the use of only one factor such as a password.

<sup>76</sup> Uses more than one factor to authenticate a user.

## Introduction to Information Security

- For example, a user with administrator privileges is authorized to access more services or resources compared to a user with non-administrator (for example, read-only) privileges.
- Authorization should be performed only if authentication is successful.

**3:**

- Refers to the logging of all transactions for the purpose of assessing the effectiveness of security mechanisms.
- Helps to validate the behavior of the infrastructure components, and to perform forensics, debugging, and monitoring activities.

## Security Concepts

### Assets

- Includes information, hardware, and software.
- Security considerations:
  - Must provide easy access to authorized users.
  - Must be difficult for potential attackers to compromise.
  - Cost of securing the assets should be a fraction of the value of the assets.

### Security Threats

- Potential attacks that can be carried out.
- Attacks can be classified as:
  - Passive attacks attempt to gain unauthorized access into the system.
  - Active attacks attempt data modifications or denial-of-service (DoS) attack.

### Security Vulnerabilities

- Weaknesses that an attacker exploits to carry out attacks.
- Three security considerations:
  - Attack surface
  - Attack vectors
  - Work factor
- Managing vulnerabilities:
  - Minimize the attack surface
  - Maximize the work factor
  - Install security controls

For more details about security considerations, click [here](#).

## Security Controls

Security controls reduce the exploitation of security vulnerabilities and any subsequent impact.

Controls are categorized as:

- **Preventive** - avoid a vulnerability from being exploited.
- **Detective** - identifies when a vulnerability has been exploited.
- **Corrective** - reduces the impact of an exploited vulnerability.

Controls can be:

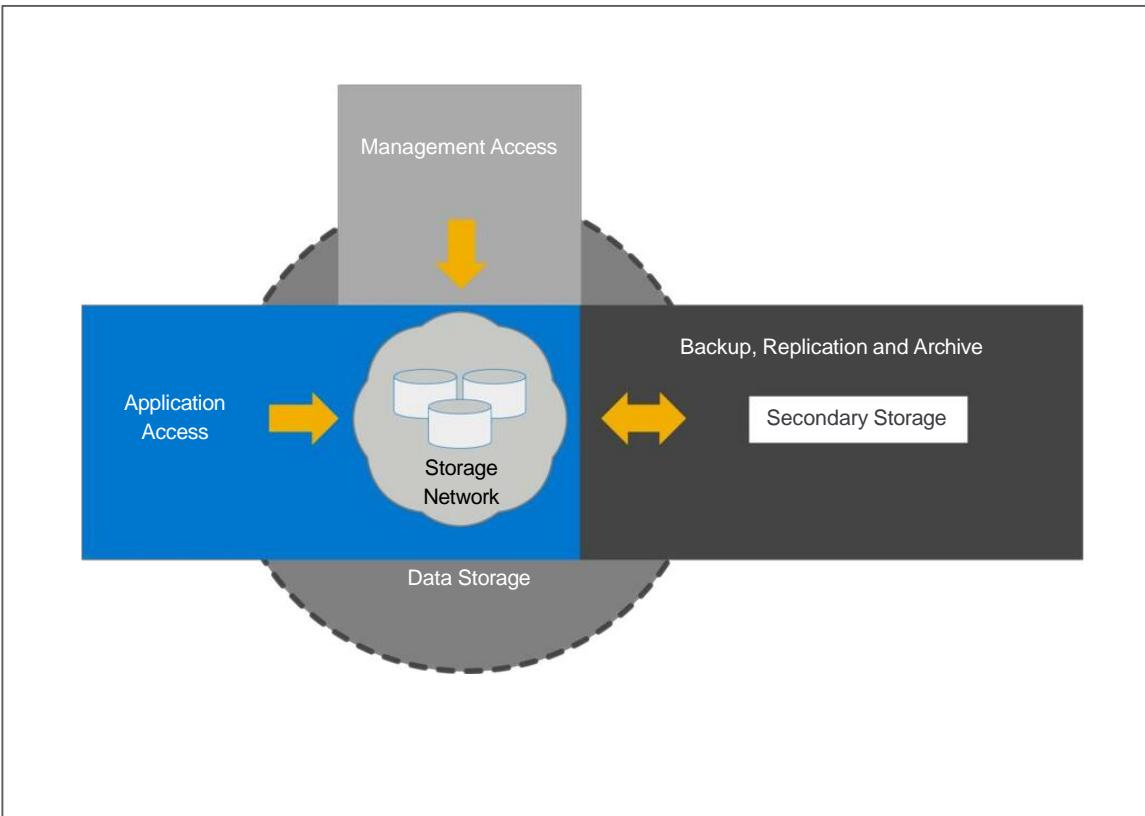
- Technical: antivirus, firewalls, and Intrusion Detection and Prevention System (IDPS)
- Non-technical: administrative policies and physical controls.

### Notes:

The three factors to consider when assessing the extent to which an environment is vulnerable to security threats are:

- **Attack surface** refers to the various entry points that an attacker can use to launch an attack, which includes people, process, and technology. For example, each component of a storage infrastructure is a source of potential vulnerability.
- **Attack vector** is a step or a series of steps necessary to complete an attack. For example, an attacker might exploit a bug in the management interface to execute a snoop attack.
- **Work factor** refers to the amount of time and effort required to exploit an attack vector.

## Storage Security Domains



*Three security domains of a storage environment (click image to enlarge)*

There are three storage security domains that must be properly secured:

- Application access<sup>77</sup>

---

<sup>77</sup> Application access domain may include only those applications that access the data through the file system or a database interface.

## Introduction to Information Security

- Management access<sup>78</sup>
- Backup, Replication and Archive<sup>79</sup>

---

<sup>78</sup> The second security domain includes management access to storage and interconnecting devices and to the data residing on those devices. Management access, whether monitoring, provisioning, or managing storage resources, is associated with every device within the storage environment.

<sup>79</sup> Primarily accessed by storage administrators who configure and manage the environment. Along with the access points in this domain, the backup and replication media also needs to be secured.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. By connecting the dots, match the following elements with their descriptions:

A.Auditing	<u>A</u>	Logging of all transactions for assessing the effectiveness of security mechanisms.
B.Compliance	<u>B</u>	Demonstrating adherence to external laws and regulations as well as to policies and procedures.
C.Authentication	<u>D</u>	Determines the purpose, strategy, and operational rules by which companies are directed and managed.
D.Governance	<u>C</u>	Process to ensure that users or assets verify their identity credentials.

## Key Security Threats

## Key Security Threats

### Denial of Service

- Prevents legitimate users from accessing resources or services.
  - Examples: Exhausting network bandwidth or CPU cycles.
  - Target compute systems, networks, and storage resources.
- Distributed DoS (DDoS) is a variant of DoS attack.
  - Several systems launch a coordinated DoS attack on target(s).
  - Attacker multiplies the effectiveness of the DoS attack by harnessing the resources of multiple collaborating attack systems.

### Malicious Insiders

A malicious insider is an organization's current or former employee, contractor, or other business partner who has or had authorized access to an organization's compute systems, network, or storage.

Control measures:

- Strict access control policies.
- Security audit and data encryption.
- Disable employee accounts immediately after separation.
- Segregation of duties (role-based access control).
- Background investigation of candidates before hiring.

## Man-in-the-middle Attack

A “man-in-the-middle” attack is another way to hack user’s credentials.

- In this attack, the attacker eavesdrops—overhears the conversation—on the network channel between two sites.
- Control measures:
  - Use of multi-factor authentication and IPsec<sup>80</sup> can prevent this type of attack.

## Account Hijacking

Account hijacking is a scenario where an attacker gains access to an administrator’s or user’s account(s).

- **Phishing** is a social engineering attack that is used to deceive users. Phishing attacks are typically carried out by spoofing email – an email with a fake but genuine-appearing address, which provides a link to a website that masquerades as a legitimate website.
    - After opening the website, users are asked to enter details such as their login credentials. These details are then captured by the attacker to take over the user’s account.
  - By **installing keystroke-logging malware**, the attacker captures the user’s credentials.
    - After capturing the credentials, an attacker can use them to gain access to the IT environment.
  - Controls measures:
- 

<sup>80</sup> A suite of algorithms, protocols, and procedures used for securing IP communications by authenticating and/or encrypting each packet in a data stream.

## Key Security Threats

- Use of multi-factor authentication, IPsec, IDPS, and firewall.

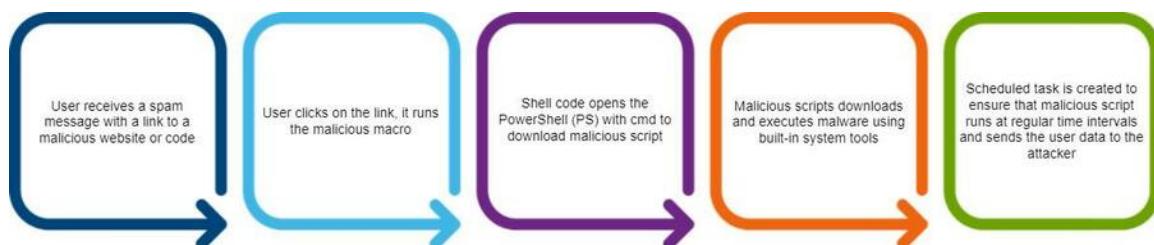
## Shared Technology Vulnerabilities

- An attacker may exploit the vulnerabilities of tools used to enable multi-tenant environments.
- Examples of threats:
  - Failure of controls that provide separation of memory and storage.
  - Hyperjacking attack involves installing a rogue hypervisor that takes control of compute system.
- Control measure:
  - Examining program memory and processor registers for anomalies.

## Fileless Attacks

Fileless attacks fall are low-observable characteristics (LOC) attacks that avoids detection by most security solutions.

- Fileless attacks are not based on new files and do not install new software on target machine.
- Fileless infections goes straight into memory and the malicious content never touches the hard drive.
- Fileless malware controls whitelisted applications that are already approved by an IT organization.
  - Example: Web browser vulnerabilities are exploited to run malicious code.



Working of Fileless attack (click image to enlarge)

## Insecure APIs

- APIs are used in modern data center environment to perform various activities such as resource provisioning, configuration, monitoring, management and orchestration.
- The attacker may exploit an API vulnerability to carry out an attack.
- Control measures:
  - Authentication, authorization, encryption, and avoiding buffer overflows.
  - Periodic security reviews of APIs.
  - Restrict access to the API only to authorized users.

Knowledge Check

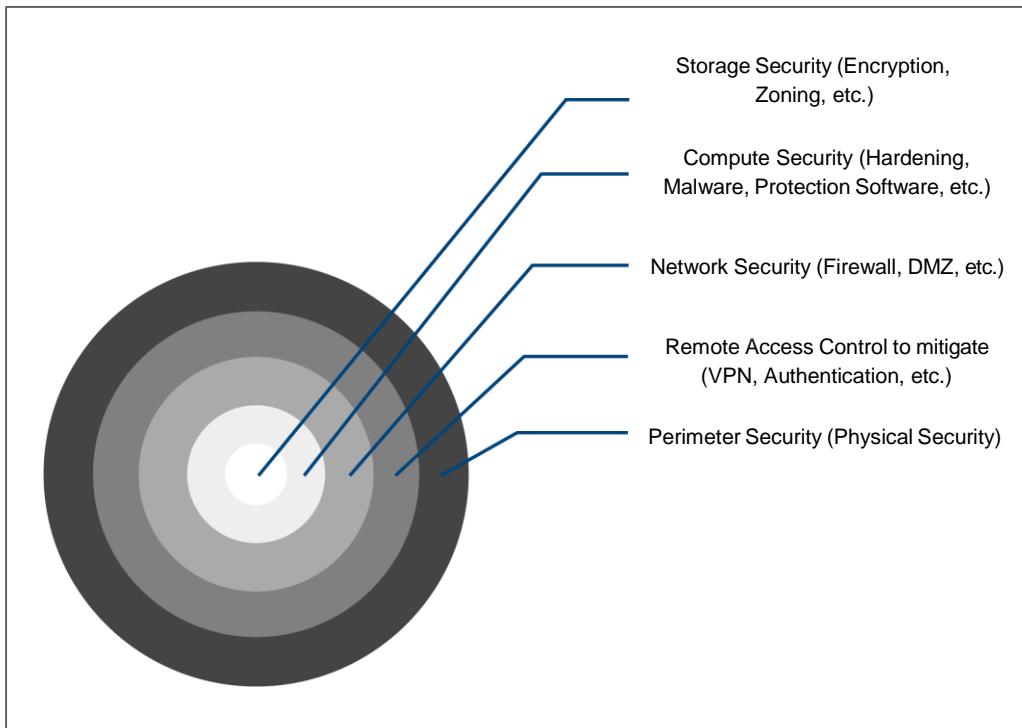
## Knowledge Check

## Knowledge Check

1. Which attack is an example of a social engineering attack that is used to deceive users?
  - a. Phishing
  - b. Man-in-the-middle
  - c. Fileless
  - d. Denial of services

## Security Controls

## Defense-in-depth



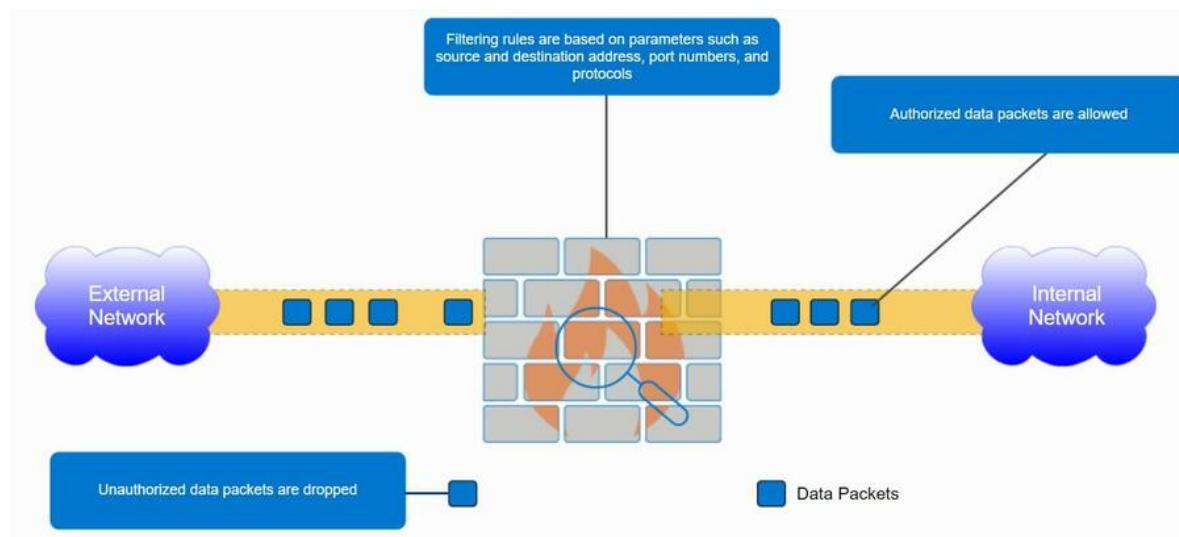
*Multilayered security mechanism for Defense-in-depth (click image to enlarge)*

A multilayered security mechanism is deployed throughout the infrastructure mitigate security risks if one layer of the defense is compromised.

- Defense-in-depth increases the barriers to exploitation.
  - An attacker must breach each layer of defense to be successful.
  - Provides additional time to detect and respond to an attack.
  - Reduces the scope of a security breach.

### Security Controls

#### Firewall



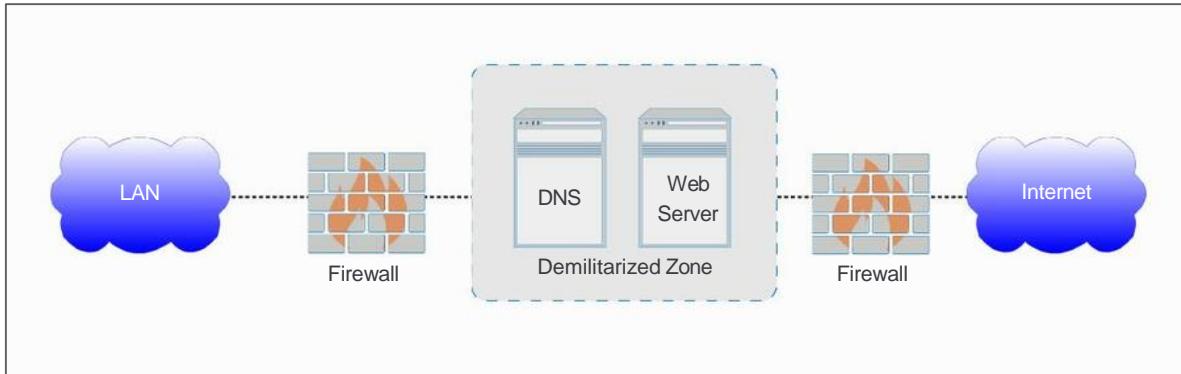
*Working of firewall (click image to enlarge)*

- A firewall is a security control designed to examine data packets traversing a network and compare them to a set of filtering rules<sup>81</sup>.
  - Rules can be set for both the incoming and the outgoing traffic.
  - Effectiveness of a firewall depends on how robustly and extensively the security rules are defined.
  - Unauthorized packets are dropped and not allowed to continue to the requested destination.

---

<sup>81</sup> A rule may use various filtering parameters such as source address, destination address, port numbers, and protocols.

## Demilitarized Zone



A DMZ between two firewalls creating safe zone between LAN and Internet (click image to enlarge)

- A demilitarized zone is a control to secure internal assets while allowing Internet-based access to selected resources.
- In a demilitarized zone environment, servers that need Internet access are placed between two firewalls.
  - Servers in the demilitarized zone may or may not be allowed to communicate with internal resources.
- Application-specific ports such as those designated for HTTP or FTP traffic are allowed through the firewall to the demilitarized zone servers.
- No Internet-based traffic is allowed to go through the second firewall and gain access to the internal network.

## IDPS

Intrusion detection is the process of detecting events that can compromise the confidentiality, integrity, or availability of IT resources.

## Security Controls

- Intrusion Detection System (IDS)<sup>82</sup> and Intrusion Prevention System (IPS)<sup>83</sup> are the two controls that usually work together and are generally referred to as intrusion detection and prevention system (IDPS).
- The key techniques used by an IDPS to identify intrusion in the environment are:
  - Signature-based detection<sup>84</sup>
  - Anomaly-based detection<sup>85</sup>

## Virtual Private Network

- A virtual private network (VPN) provides a secure connection to the IT resources. In the modern data protection environment, VPN is used to provide:
  - Secure site-to-site connection between a primary site and a DR site when performing remote replication.
  - Secure site-to-site connection between an organization's data center and cloud when performing cloud-based backup and replication.
- There are two methods in which a VPN connection can be established:
  - Remote access VPN connection<sup>86</sup>

---

<sup>82</sup> A security tool that automates the detection process. An IDS generates alerts, in case anomalous activity is detected.

<sup>83</sup> A tool that has the capability to stop the events after they have been detected by the IDS.

<sup>84</sup> IDPS relies on a database that contains known attack patterns or signatures, and scans events against it.

<sup>85</sup> IDPS scans and analyzes events to determine whether they are statistically different from events normally occurring in the system.

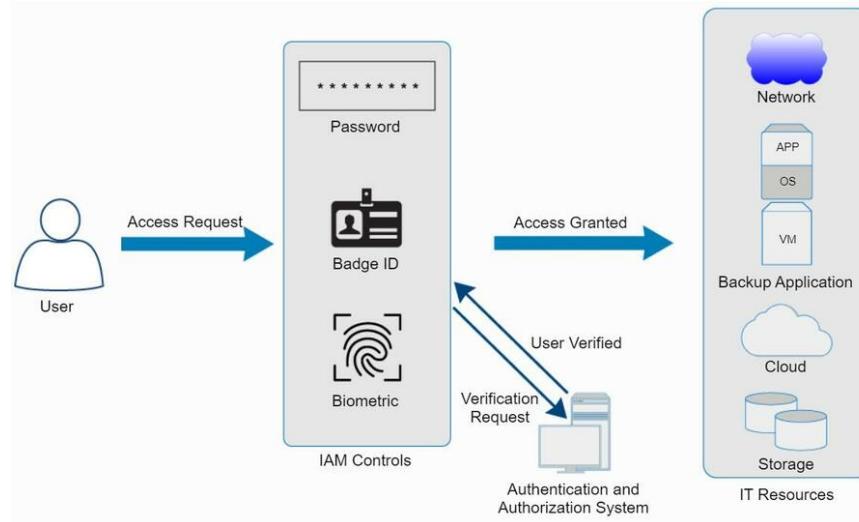
- Site-to-site VPN connection<sup>87</sup>

---

<sup>86</sup> A remote client (typically client software installed on the user's compute system) initiates a remote VPN connection request. A VPN server authenticates and provides the user access to the network.

<sup>87</sup> The remote site initiates a site-to-site VPN connection. The VPN server authenticates and provides access to internal network.

### Identity and Access Management (IAM)



*Identity and Access Management Process (click image to enlarge)*

- Identity and access management (IAM) is the process of:
  - Managing user's identifiers and their authentication and authorization to access IT infrastructure resources.
  - Controlling access to resources by placing restrictions based on user identities.
  - Identifying the user and the privileges assigned to the user.

#### Notes: IAM Example

- A user tries to gain access to the IT resources. While doing so:
  - The IAM controls prompt for the user's credentials.
  - The user enters the requested credentials such as user\_id and password.
  - Credentials are then verified against a system that has the ability to authenticate and authorize the user.
  - Upon successfully verifying the credentials, the authorized user is granted access to the IT resources.

## Multifactor Authentication

Multifactor authentication uses more than one factor to authenticate a user.

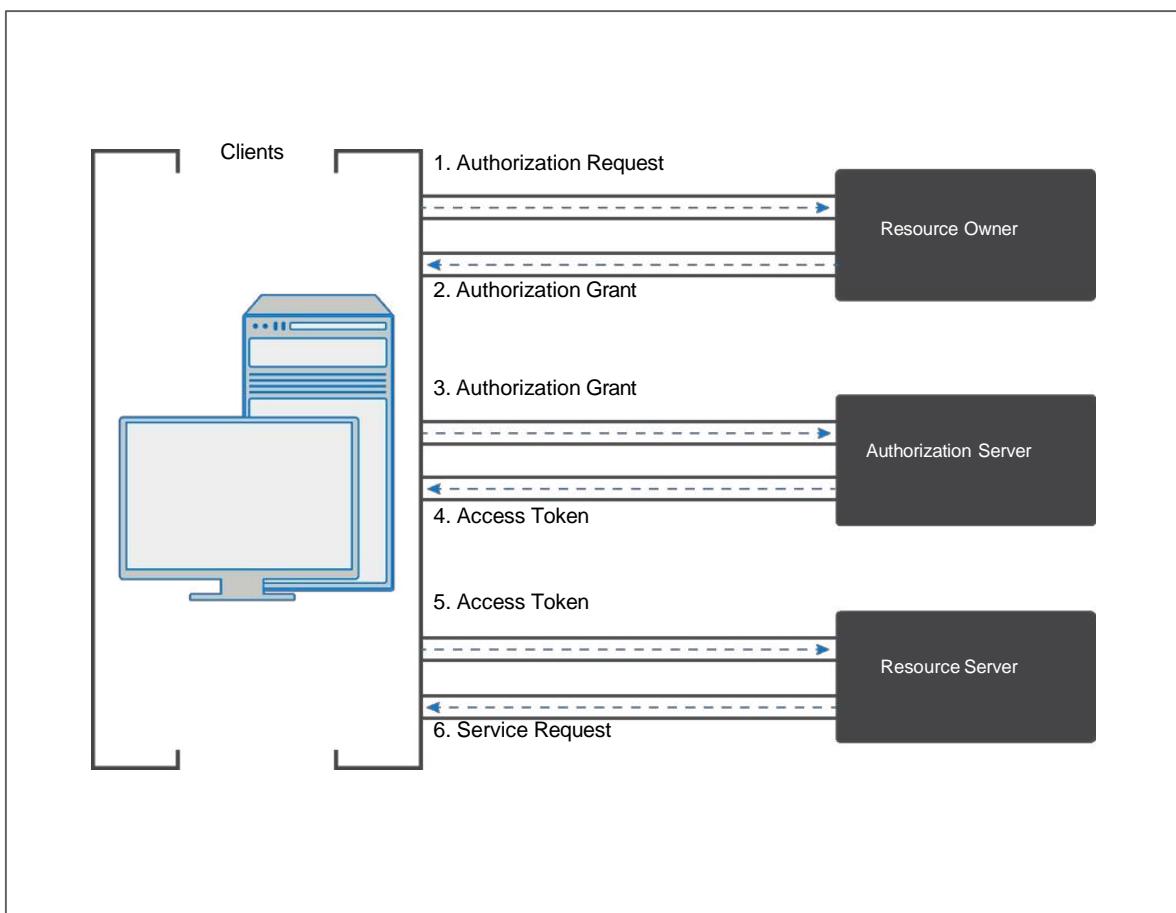
- A common two-factor authentication requires a user to enter a password and a token-generated passcode.
- Thus, if the password is stolen, then access would not be granted without the passcode.



*Multifactor authentication to authenticate a user (click image to enlarge)*

### OAuth and OpenID

#### OAuth



*Open Authorization (OAuth) Process (click image to enlarge)*

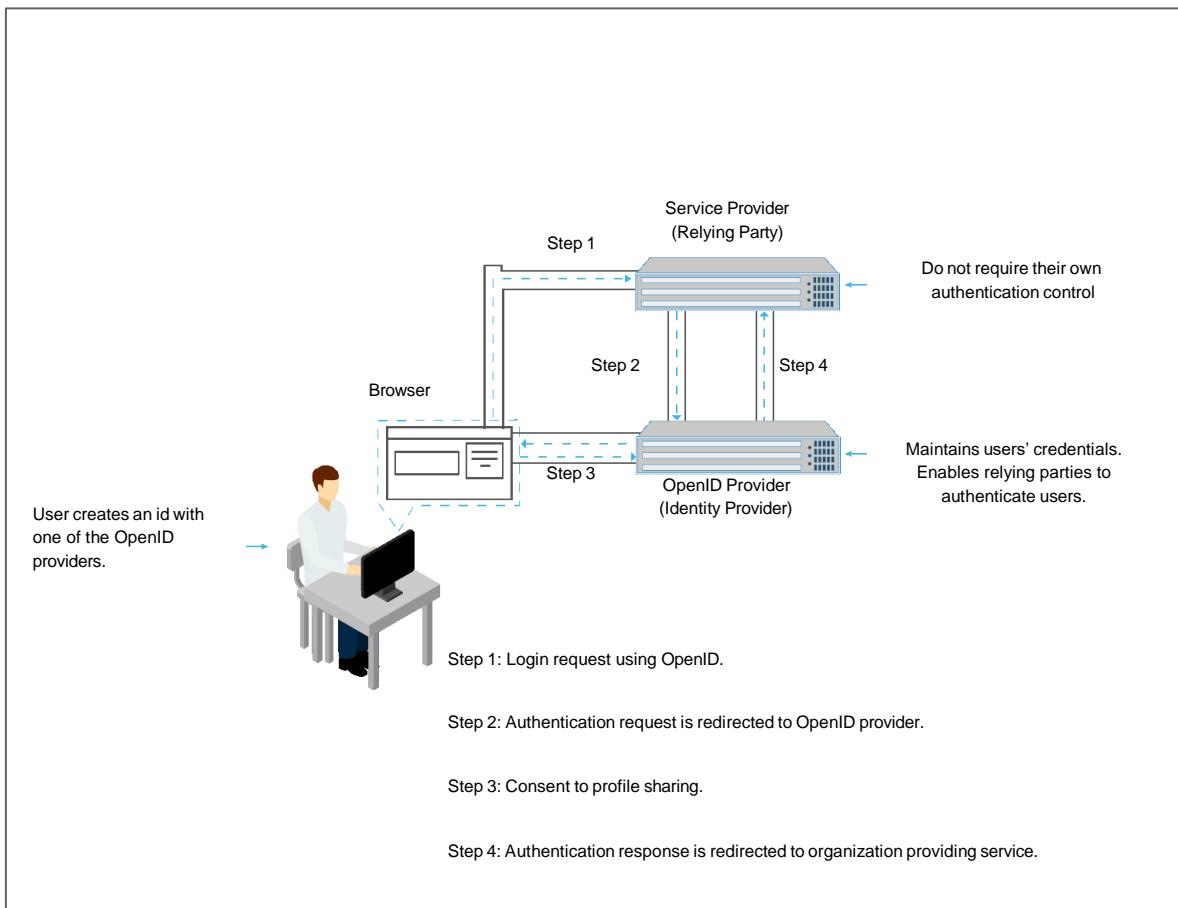
An open authorization control enables a client to access protected resources from a resource server on behalf of a resource owner.

- Can be used to secure application access domain.
  - Example: Giving LinkedIn permission to access your Facebook contacts.
- There are four entities involved in the authorization control:
  - Resource owner
  - Resource server
  - Client

- Authorization Server

For more information about the OAuth process as shown in the image, click [here](#).

## OpenID



*OpenID implementation process*

## Security Controls

OpenID is an open standard for authentication in which an organization uses authentication services from an OpenID third-party provider.

- The organization is known as the relying party and the OpenID provider<sup>88</sup> is known as the identity provider.
- The user creates an OpenID with an OpenID provider. This OpenID can be used to sign on to any organization (relying party) that accepts OpenID authentication.
- Control can be used in the modern environment to secure application access domain.

### Notes: OAuth

The image shows the steps involved in OAuth process as described in Request for Comments (RFC) 6749 published by Internet Engineering Task Force (IETF):

1. The client requests authorization from the resource owner. The authorization request can be made directly to the resource owner, or indirectly through the authorization server.
  2. The client receives an authorization grant, which is a credential representing the resource owner's authorization to access its protected resources. It is used by the client to obtain an access token. Access tokens are credentials that are used to access protected resources. An access token is a string representing an authorization issued to the client. The string is usually opaque to the client.
- 

<sup>88</sup> An OpenID provider maintains users credentials on their authentication system and enables relying parties to authenticate users requesting the use of the relying party's services. This eliminates the need for the relying party to deploy their own authentication systems.

Tokens represent specific scopes and durations of access, granted by the resource owner, and enforced by the resource server and authorization server.

3. The client requests an access token by authenticating with the authorization server and presenting the authorization grant.
4. The authorization server authenticates the client and validates the authorization grant, and if valid, issues an access token.
5. The client requests the protected resource from the resource server and authenticates by presenting the access token.
6. The resource server validates the access token, and if valid, serves the request.

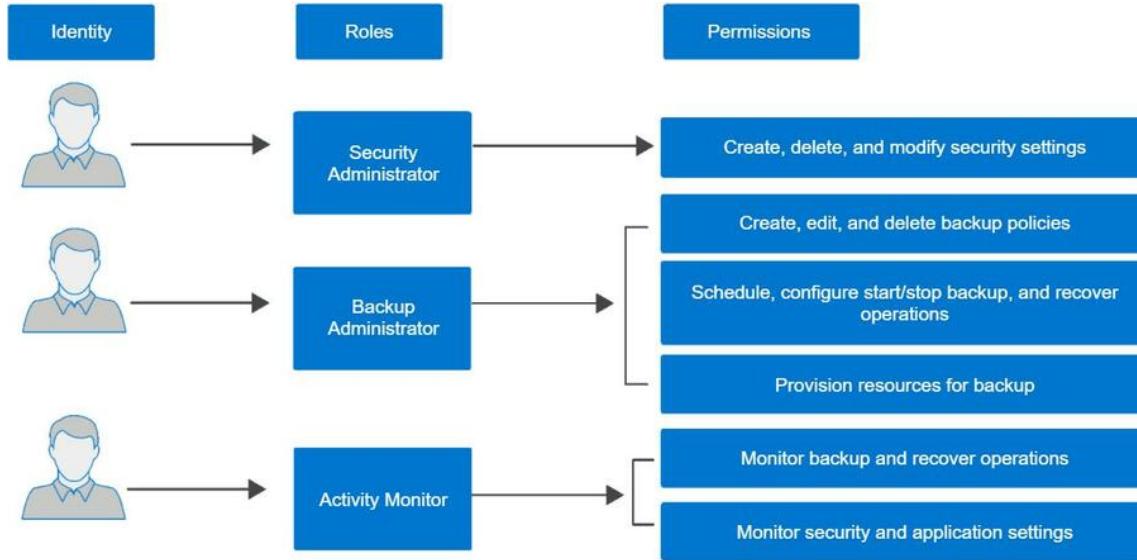
#### **Notes: OpenID**

The image shows the OpenID concept by considering a user who requires services from the relying party.

1. For the user to use the services provided by the relying party an identity (user ID and password) is required.
2. The relying party does not provide their own authentication control, however they support OpenID from one or more OpenID providers.
3. The user can create an ID with the identity provider and then use this ID with the relying party.
4. The relying party, after receiving the login request, authenticates it with the help of identity provider and then grants access to the services.

## Security Controls

### Role-Based Access Control



*Implementation of RBAC in a data protection environment*

- Role-based access control (RBAC) is an approach to restrict access to the authorized users based on their respective roles<sup>89</sup>.
  - Minimum privileges are assigned to a role that is required to perform the tasks associated with that role.
- Always consider administrative controls, such as separation of duties<sup>90</sup>, when defining the data center security procedures.

---

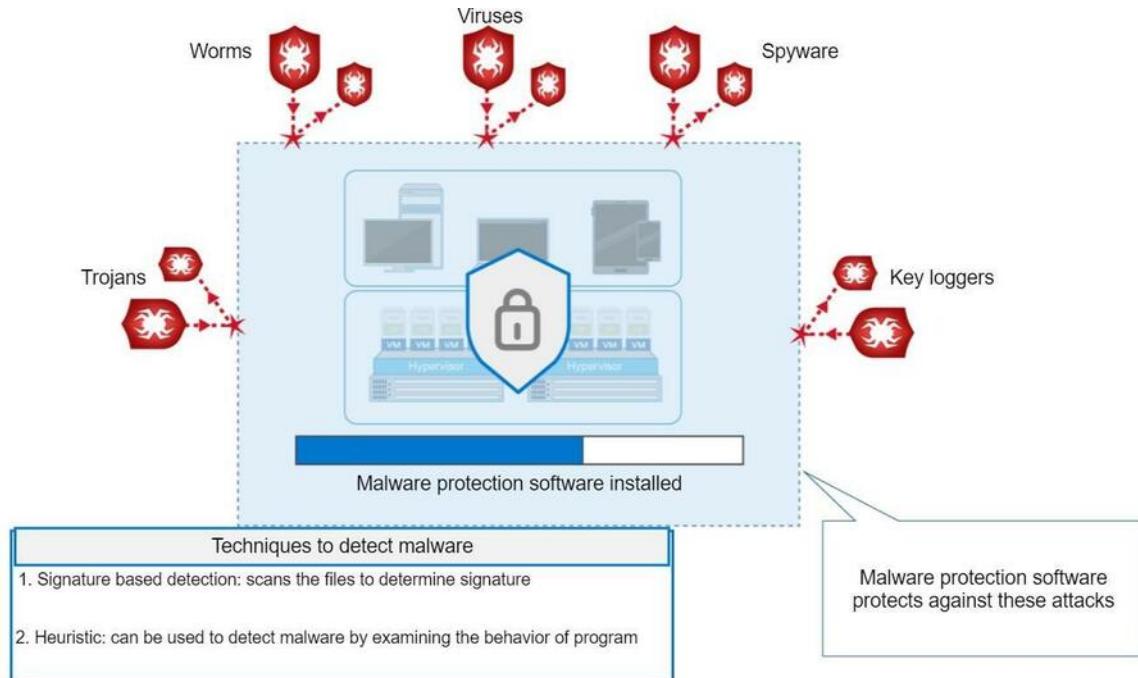
<sup>89</sup> A role may represent a job function, for example a backup administrator.

<sup>90</sup> Clear separation of duties ensures that no individual can both specify an action and carry it out.

## Security Controls

- For example, the person who authorizes the creation of administrative accounts in a data protection environment should not be the person who uses those accounts.

### Malware Protection Software



#### *Implementation of malware protection software*

- Installed on a compute system or mobile device, malware protection software:
  - Detects, prevents, and removes malware and malicious programs such as viruses, worms, trojan horses, key loggers, and spyware.
  - Uses various techniques to detect malware.

- Most common techniques used is signature-based detection<sup>91</sup>.
- Identifies malware by examining the behavior of programs.

---

<sup>91</sup> In this technique, the malware protection software scans the files to identify a malware signature.

## Mobile Device Management

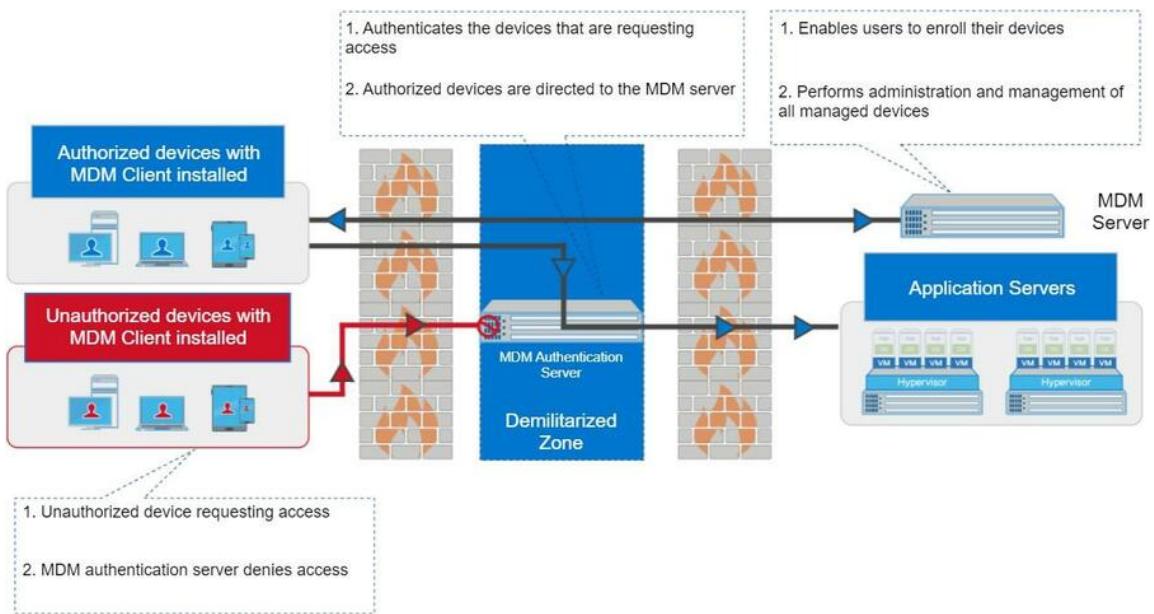
- Several organizations allow their employees to access organization's internal application and resources via mobile devices.
  - Introduces a threat that may expose resources to an attacker.
- Mobile device management (MDM) is a control that restricts access to organization's resources only to authorized mobile devices.
- MDM solution consists of two components: the server component<sup>92</sup> and the client component<sup>93</sup>.
- MDM solution enables organizations to enforce organization's security policies on the user's mobile devices.

---

<sup>92</sup> Responsible for performing device enrollment, administration, and management of mobile devices.

<sup>93</sup> Installed on the mobile device that needs access to the organization's resources. The client receives commands from the server component which it executes on the mobile device.

## Security Controls



*Implementation of mobile device management*

### Data Encryption



- Data encryption is a cryptographic technique in which data is encoded and made indecipherable to eavesdroppers or hackers.
- Provides protection from threats such as:
  - Tampering with data which violates data integrity.
  - Media theft which compromises data availability.
  - Sniffing attacks which compromise confidentiality.
- Data encryption is one of the most important controls for securing data in-flight<sup>94</sup> and at-rest<sup>95</sup> in a modern data center environment.

#### Notes:

---

<sup>94</sup> Refers to data that is being transferred over a network.

<sup>95</sup> Refers to data that is stored on a storage medium.

- Data should be encrypted as close to its origin as possible. Data encryption:
  - Can be used for encrypting data at the point of entry into the storage network.
  - Can be implemented on the fabric to encrypt data between the compute system and the storage media. These controls can protect both the data at-rest on the destination device and the data in-transit.
  - Can be deployed at the storage-level, which can encrypt data-at-rest.
- Another way to encrypt network traffic is by using cryptographic protocols such as Transport Layer Security (TLS) which is a successor to Secure Socket Layer (SSL).
  - These are application layer protocols and provide an encrypted connection for client-server communication.
  - These protocols are designed to prevent eavesdropping and tampering of data on the connection over which it is being transmitted.

## Data Shredding

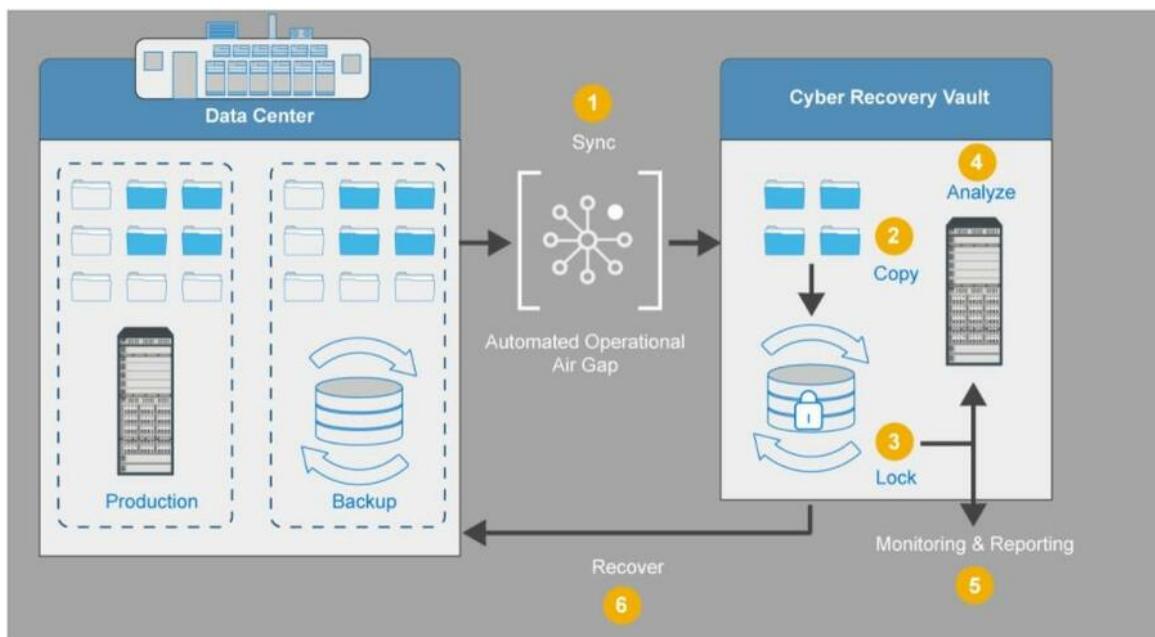
- A process of deleting data or residual representations of data which makes it unrecoverable.
- When data is deleted, sometimes the actual strings of binary data may remain on the storage device.
- On magnetic media, magnetic residuals (remanence) can remain after deleting data.

<b>Data Shredding Techniques</b>	<b>Description</b>
Physically destroying	Damaging the storage media physically.
Degaussing	Process of decreasing or eliminating the magnetic field of media.
Overwriting	Data on the disk or flash drives can be shredded by overwriting the disks several times with invalid data.

## Cyber Recovery

- True information protection emphasizes keeping an isolated copy of your critical data such as essential applications and intellectual property off the network.
- Cyber recovery architecture:
  - Maintains critical business data and technology configurations in a secure, air-gapped 'vault' environment that can be used for recovery or analysis.
  - Isolates data to ensure an uncompromised copy always exists.
  - Creates point-in-time (PIT) retention-locked copies that can be validated and then used for recovery of the production system.

Synch-Copy-Lock operation of data protection and vaulting process



**1:** Security mechanism that involves isolating a network and preventing it from establishing an external connection.

**2:** Creates point-in-time copies that can serve as restore points in case production backup data is subject to destructive cyberattack.

Synchronizes the latest data, creates a copy, and then secures it.

## Security Controls

**3:** Immutable file locking and secure data retention to meet both corporate governance and compliance standards.

**4:** Determines if a replication copy contains malware or other anomalies that must be removed.

**5:**

- Provides comprehensive alerting and reporting that enable administrators to monitor ongoing activities.
- Detects affected copies, and alert is sent and actions must be taken to resolve the problems that might occur.

**6:** The data in a point-in-time copy can be re-orchestrated and then used to replace the lost data in production.

## Penetration Testing

Penetration testing evaluates systems, networks, and applications to find vulnerabilities and threats that an attacker could exploit.

Penetration testing is performed through several stages as shown in the image.

Stages of penetration testing



**1:** First stage includes goals and priorities of an organization. Investigation includes collecting information about active and passive network, domains and mails of the target system or network.

**2:** Second stage is to examine and test the system, network, and application against attacks and automated intrusion attempts.

**3:** Third stage checks the compromised system or network, and application by identifying the exploited vulnerabilities.

**4:** Fourth stage collects the evidence of the exploited vulnerabilities and determines if persistence access can be maintained.

**5:** In the fifth stage, the identified findings are documented:

- Approvals made in previous stages
- Risk levels by exploited vulnerabilities
- Sensitive data that was breached
- Total engaged time of pen-tester
- Final recommendations for future security

## VM, OS and Application Hardening

### Virtual Machine (VM) Hardening



*Virtual machine hardening*

Virtual machine hardening includes:

- Change the default configuration of the VM.
- Disconnection of the virtual components that are not required.
- Ensuring that the security mechanisms are enabled, and are up-to-date.
- Isolation of the VM network using VLANs.
- Creation of the virtual machine from the VM template.

## Operating System (OS) Hardening



*Operating system hardening*

Operating system hardening includes:

- Deletion of unused files and programs.
- Installation of current OS updates and patches.
- Performing vulnerability scanning and penetration testing.

## Application Hardening



*Application hardening*

Application hardening checklist includes:

- Identify security policies and procedures.

## Security Controls

- Examine transmission of credentials over the network.
- Implement access control list (ACL) to restrict applications.
- Secure third party applications and tools.
- Install application updates or patches.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. Which statement is true when implementing RBAC?
  - a. An individual can both specify an action and carry it out.
  - b. Maximum privileges are assigned to a role to perform multiple tasks.
  - c. No individual can both specify an action and carry it out.
  - d. An auditing role can create and delete the security settings.

## Knowledge Check

2. What is the purpose of having point-in-time replication copies in the cyber recovery vault?
  - a. Enable restore points if production data is jeopardized.
  - b. Provides ability to quickly scale to meet growing end-user demands.
  - c. Determine if copy contains malware or anomalies.
  - d. Provide comprehensive alerting and reporting to monitor activities.

## Concepts in Practice

## Concepts in Practice

### Dell EMC CloudLink

CloudLink provides multiple data encryption options across a broad spectrum of operating platforms including bare-metal, virtualized, and containerized workloads across public and private clouds, simplifying and streamlining security workflows.

Dell EMC CloudLink helps you protect your data by providing:

- Comprehensive encryption and key management.
- Support for VMware, Microsoft and Amazon Web Services environments.
- Support for Containerized applications.
- Ease of use with a single management interface and REST APIs.

CloudLink is a certified VMware Ready™ Key Management Server (KMS), giving customers granular control of VMs and data.

### Dell Change Auditor

- Helps customers to audit, alert, protect and reports user activity and configuration and application changes against Active Directory and Windows applications.
- The software has role-based access, enabling auditors to have access to only the information they need to quickly perform their job.
- Change Auditor provides visibility into enterprise-wide activities from one central console, enabling customers to see how data is being handled.

### Dell In Trust

An IT data analytics solution that provides organizations the power to search and analyze vast amounts of data in one place.

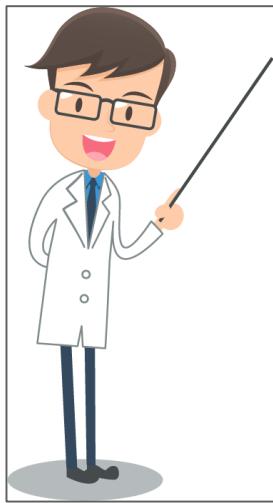
- Provides real-time insights into user activity across security, compliance, and operational teams.
- Helps administrators to troubleshoot issues by conducting security investigations regardless of how and where the data is stored.

## Concepts in Practice

- Helps compliance officers to produce reports validating the compliance across multiple systems.
- Provides information on who accessed the data, how was it obtained and how the data was used.
  - This helps administrators and security teams to discover suspicious event trends.

## Exercise - Storage Infrastructure Security

## Exercise: Storage Infrastructure Security



### Scenario

A large multinational bank:

- Provides mobile banking to its customers that enables them to access the application and data from any location.
- Enables their employees to access internal banking applications using mobile devices.
- Has multiple remote/branch offices.
- Offers single factor authentication solution.
- Sends physical tape media to an offsite location.
- Performs remote replication between the primary site and the secondary site for DR.

### Challenges

- Mobile device theft may expose resources to an attacker.
- Difficulty in tracking anomalous activity in the data center.
- Sending tapes to offsite locations would increase the risk of losing sensitive data in transit.
- Data is exposed to attackers when data is replicated between the primary site and the secondary site for DR.
- An attack was attempted by exploiting loophole in the hypervisor management system.

### Requirements

- Need to protect the confidentiality of data if employee's mobile device theft occurs.
- Requires security controls to identify anomalous activity.

## Exercise - Storage Infrastructure Security

- Need to protect data on tapes when sending tapes to offsite location.
- Need to protect data when performing replication between sites.
- Need to have security controls to protect hypervisor management system.

### Deliverables

- Propose a solution that will address the organization's challenges and requirements.

### Solutions

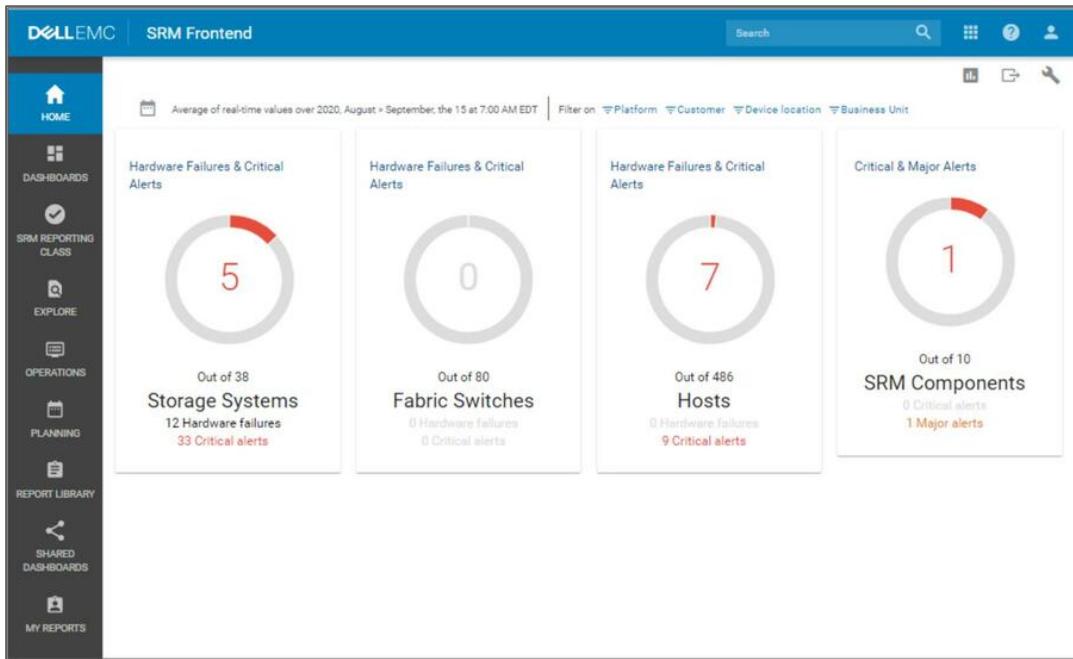
- Implement Mobile Device Management (MDM).
- Implement intrusion detection and prevention system (IDPS).
- Implement data encryption at rest and in flight.
  - Encrypt data at rest for tapes.
  - Encrypt data in flight for remote replication.
- Implement hypervisor management security controls.
  - Perform hypervisor hardening based on CIS and DISA best practices.
  - Perform security-critical hypervisor management updates.
  - Implement separate firewall with strong filtering rules.

# Storage Infrastructure Management

## Storage Infrastructure Management

## Storage Infrastructure Management

## Overview



Dell EMC Storage Resource Manager (SRM) console

Storage infrastructure management ensures the proper and cost-effective use of the available storage resources to meet the business needs.

- Helps IT organizations to achieve their strategic business goal and service level requirements.
- Aligns the storage resources with the performance needs of the applications.
- Ensures better utilization of the existing storage resources to reduce unnecessary infrastructure investments.

## Key Characteristics of Modern Storage Infrastructure Management

### Service-focused approach

Modern storage infrastructure management has a service-based focus. It is linked to the service requirements and service level agreement (SLA)<sup>96</sup>. Examples include:

- Determining the optimal amount of storage space needed in a backup storage system to meet the capacity requirement of a service.
- Creating a disaster recovery plan to meet the recovery time objective (RTO) of services.
- Ensuring that the management processes, management tools, and staffing are appropriate to provide a data archiving service.

### Software-defined data center-aware

- Software-defined data center management is more efficient over hardware-specific management.
- Many common, repeatable, hardware-specific management tasks are automated. Management is focused on strategic, value-driven activities.
- Management functions move to an external software controller.
- Management operations become independent of underlying hardware.

---

<sup>96</sup> An SLA is a formalized contract document that describes service level targets, service support guarantee, service location, and the responsibilities of the service provider and the user. These parameters of a service determine how the components of the data protection environment will be managed.

## End-to-end visibility

- Provides detailed information on configuration, connectivity, capacity, performance, and interrelationships between components.
- Enables report consolidation, correlating issues to find root-cause, and tracking migration of data and services.

## Orchestrated operations

- SDDC controller/orchestrator programmatically integrates and sequences component functions into workflows.
- Orchestrator triggers an appropriate workflow upon receiving a service provisioning or management request.
- Orchestration reduces service provisioning time, risk of manual errors, and administration cost.

## Key Storage Management Functions

### Infrastructure Discovery

- Discovery provides visibility into each infrastructure component.
  - Discovered information helps in monitoring and management.
- Discovery tool interacts and collects information from components.
- Discovery is typically scheduled to occur periodically.
  - May also be initiated by an administrator or triggered by an orchestrator.

### Monitoring, Alerts and Reporting

- Monitoring provides visibility into the storage infrastructure and forms the basis for performing management operations.
- Alerting provides information about events or impending threats or issues.
- Reporting involves gathering information from various components and operations management processes.

### Operations Management

- Operations management involves on-going management activities to maintain the IT infrastructure and the deployed services.
- Ensures that the services and service levels are delivered as committed. Operations management involves several management processes.
- Ideally, operations management should be automated to ensure the operational agility.
  - Management tools are usually capable of automating many management operations.
- Further, the automated operations of management tools can also be logically integrated and sequenced through orchestration.

# Operations Management

## Monitoring



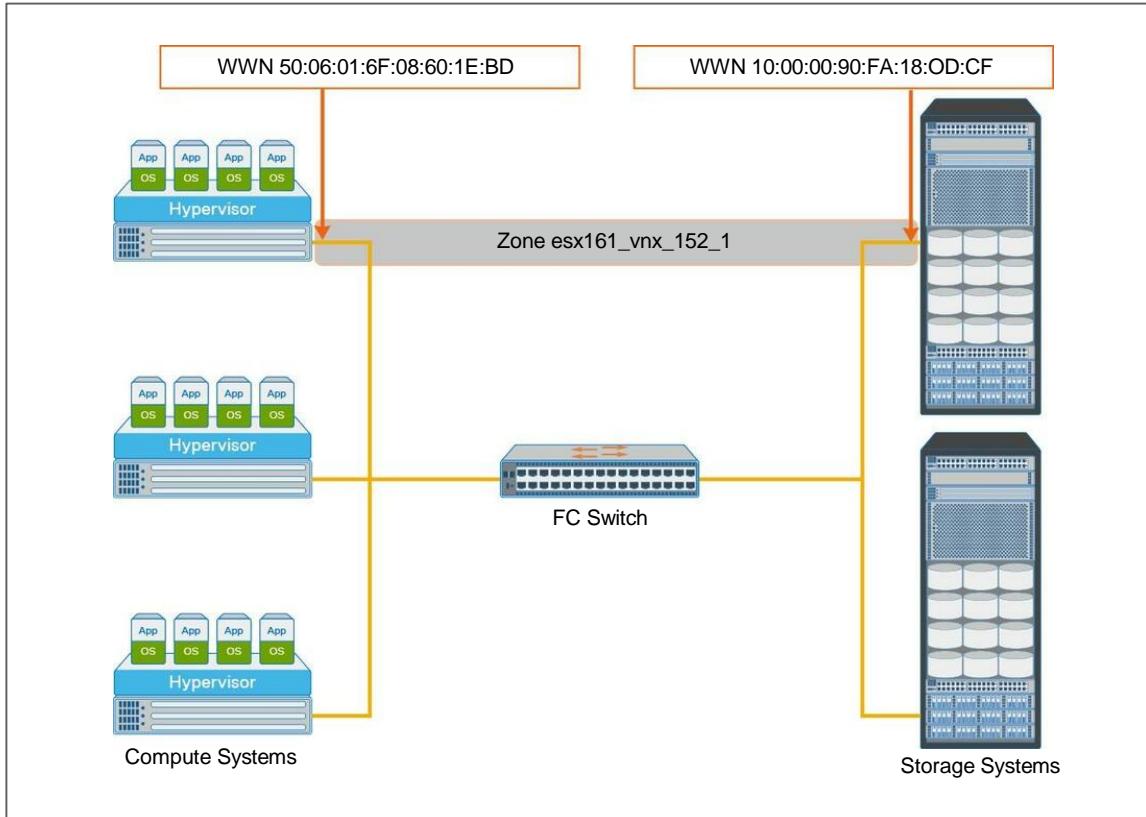
Monitoring provides visibility into the storage information health and involves the following activities:

- Tracks the performance and availability status of components and services.
- Measures the utilization and consumption of resources.
- Tracks environmental parameters such as heating, ventilating, and air-conditioning (HVAC).
- Triggers alerts when thresholds are reached, security policies are violated, or service performance deviates from SLA.

## Monitoring Parameters

Storage infrastructure is primarily monitored for:

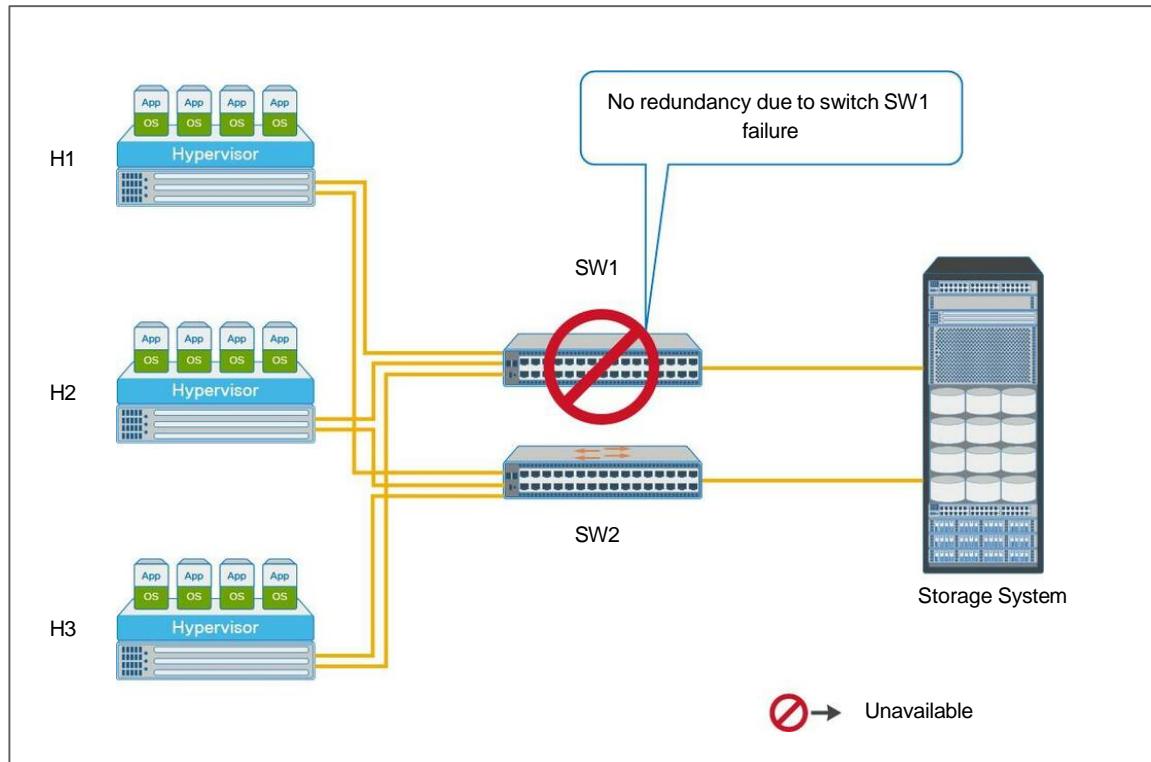
### Configuration



*Monitoring configuration changes*

- Involves tracking configuration changes and deployment of storage infrastructure components and services.
- Detects configuration errors, non-compliance with configuration policies, and unauthorized configuration changes.

## Availability

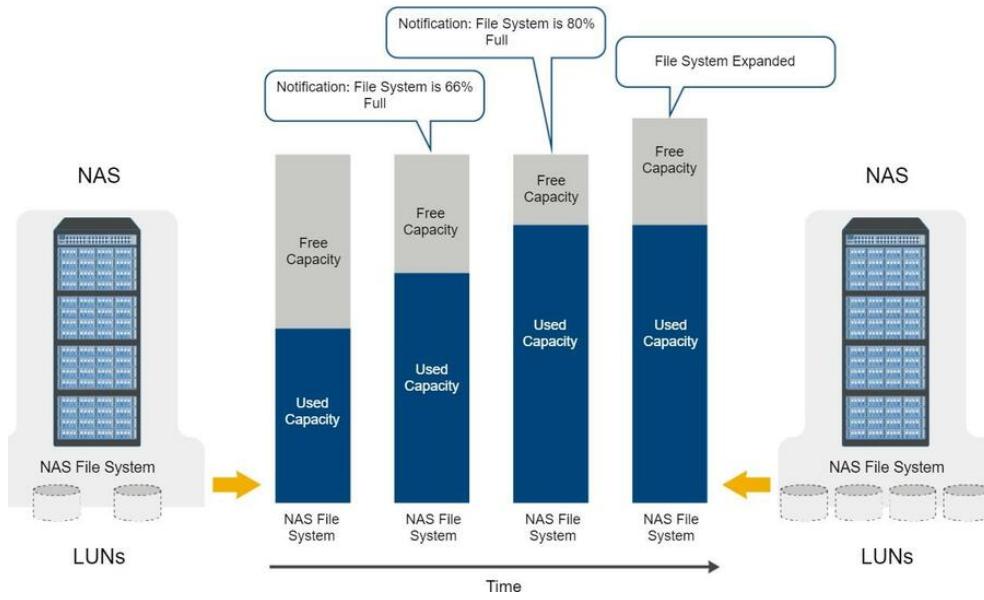


*Monitoring the availability of storage infrastructure components*

Monitoring availability of hardware components (for example, a port, an HBA, or a storage controller) or software components (for example, a database instance, an SDDC controller, or an orchestration software):

- Involves monitoring the errors generated by the infrastructure components.
- Identifies the failure of any component that may lead to data and service unavailability or degraded performance.

## Capacity



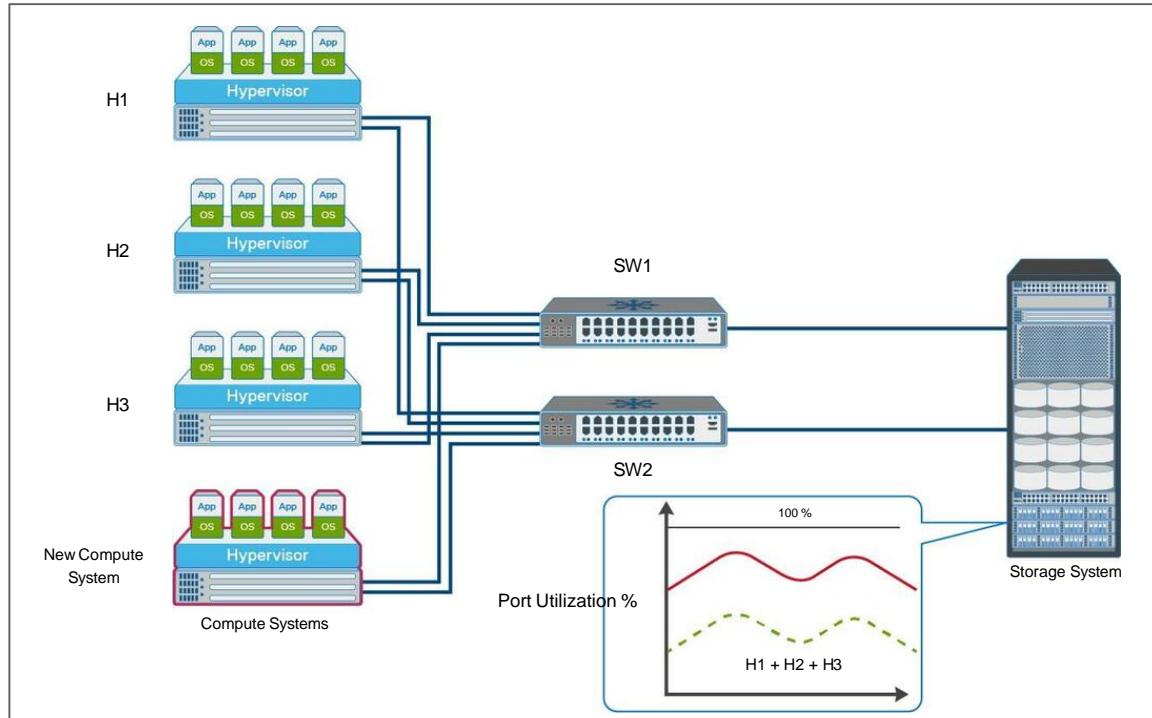
*Monitoring NAS file system capacity*

Inadequate capacity leads to degraded performance or even service unavailability.

Monitoring capacity:

- Involves examining the amount of infrastructure resources used and usable such as the free space available on a file system or a storage pool or, the numbers of ports available on a switch.
- Helps an administrator to ensure uninterrupted data availability by averting outages before they occur.

## Performance

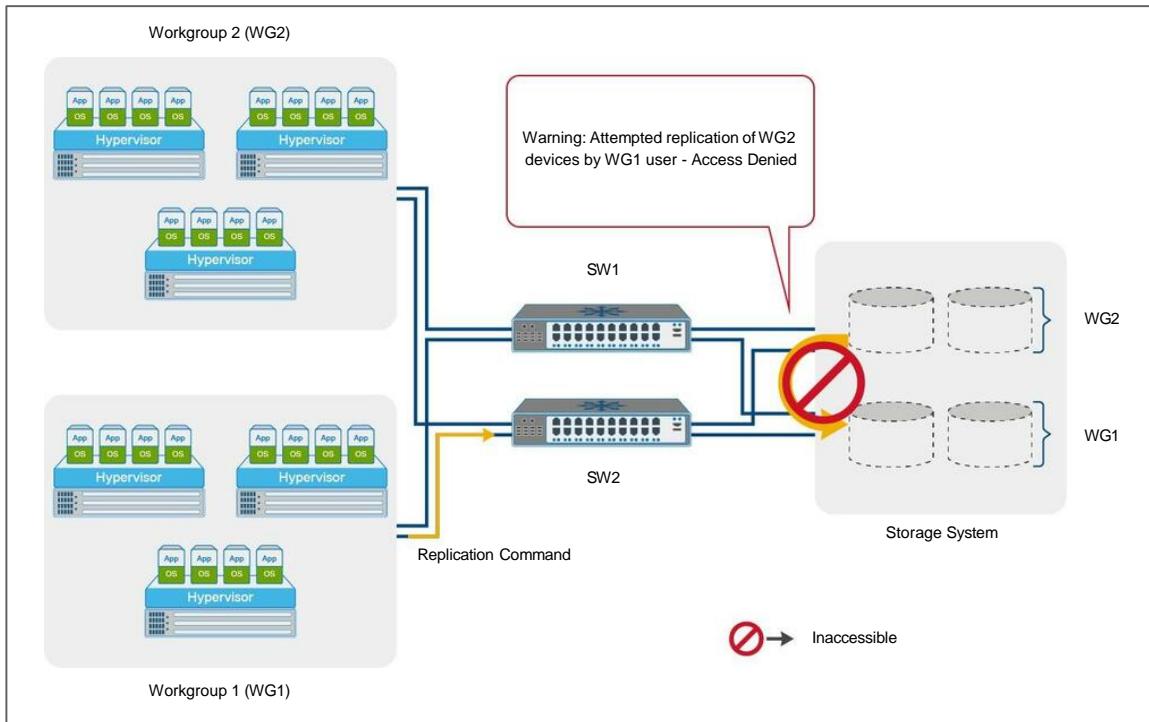


*Monitoring performance on iSCSI storage systems*

Performance monitoring tracks how efficiently different IT components and services are performing and helps to identify bottlenecks. Performance monitoring:

- Measures and analyzes behavior in terms of number of completed and failed operations per hour, amount of data backed up daily, I/O throughput.
- Identifies whether the behavior of components and services meets the acceptable performance levels.

## Security



*Monitoring security in a storage system*

Monitoring storage infrastructure for security includes tracking unauthorized access and identifying any malicious configuration changes. For example, monitoring tracks and reports the initial zoning configuration performed in an FC SAN and all the subsequent changes. Monitoring security:

- Detects all operations and data movement that deviate from predefined security policies.
- Detects unavailability of information and services to authorized users due to security breach.

### Notes: Monitoring Configuration

The image illustrates an example of configuration changes in the storage infrastructure. In this example:

- The configuration changes are captured and reported by a monitoring tool in real-time.

## Operations Management

- A new zone is created to enable a compute system to access LUNs from one of the storage systems.
- The changes are made on the FC switch (device).

The table lists configuration changes in the storage infrastructure.

Changed At	Description	Device	Compliance Breach
2021/01/07 @ 13:34:23	The member 10000090FA180DCF has been added to the zone esx161_vnx_152_1	100000051E023364	No
2021/01/07 @ 13:34:23	The member 5006016F08601EBD has been added to the zone esx161_vnx_152_1	100000051E023364	No
2021/01/07 @ 13:34:23	A new zone esx161_vnx_152_1 has been added to the fabric 100000051E023364	100000051E023364	No

### Notes: Monitoring Availability

The image illustrates an example of monitoring the availability of storage infrastructure components, including:

- A storage infrastructure includes three compute systems (H1, H2, and H3) that are running hypervisors.
- All the compute systems are configured with two FC HBAs, each connected to the production storage system through two FC switches, SW1 and SW2. All the compute systems share two storage ports on the storage system.

- Multipathing software has also been installed on hypervisor running on all the three compute systems. If one of the switches, SW1 fails, the multipathing software initiates a path failover, and all the compute systems continue to access data through the other switch, SW2.
- Due to absence of redundant switch, a second switch failure could result in unavailability of the storage system. Monitoring for availability enables detecting the switch failure and helps administrator to take corrective action before another failure occurs. In most cases, the administrator receives symptom alerts for a failing component and can initiate actions before the component fails.

### **Notes: Monitoring Capacity**

The image illustrates the importance of monitoring the capacity of a storage pool in a NAS system:

- If the file system is full and no space is available for applications to perform write I/O, it may result in application/service outage.
- Monitoring tools can be configured to issue a notification when thresholds are reached on the file system capacity; for example:
  - When the file system reaches 66 percent of its capacity, a warning message is issued.
  - A critical message is issued when the file system reaches 80 percent of its capacity.
  - This enables the administrator to take actions to provision additional LUNs to the NAS and extend the NAS file system before it runs out of capacity.

### **Notes: Monitoring Performance**

The image provides an example that illustrates the importance of monitoring performance on iSCSI storage systems; in this example:

- Compute systems H1, H2, and H3 (with two iSCSI HBAs each) are connected to the storage system through Ethernet switches SW1 and SW2.
- The three compute systems share the same storage ports on the storage system to access LUNs.

## Operations Management

- A new compute system running an application with a high work load must be deployed to share the same storage port as H1, H2, and H3.
- Monitoring storage port utilization ensures that the new compute system does not adversely affect the performance of the other compute systems.

Here, utilization of the shared backup storage system port is shown by the solid and dotted lines in the graph. If the port utilization prior to deploying the new compute system is close to 100 percent, then deploying the new compute system is not recommended because it might impact the performance of the backup clients running on other compute systems. However, if the utilization of the port prior to deploying the new compute system is closer to the dotted line, then there is room to add a new compute system.

### **Notes: Monitoring Security**

The image illustrates the importance of monitoring security in a storage system. In this example:

- The storage system is shared between two workgroups, WG1 and WG2.
- The data of WG1 should not be accessible by WG2 and vice versa.
- A user from WG1 might try to make a local replica of the data that belongs to WG2.
- If this action is not monitored or recorded, it is difficult to track such a violation of security protocols.
- Conversely, if this action is monitored, a warning message can be sent to prompt a corrective action or at least enable discovery as part of regular auditing operations.

## Alerts

An **alert** is a system-to-user notification that provides information about events or impending threats or issues. Alerting keeps administrators informed about the status of various components and operations, which can impact the availability of services and require immediate administrative attention such as:

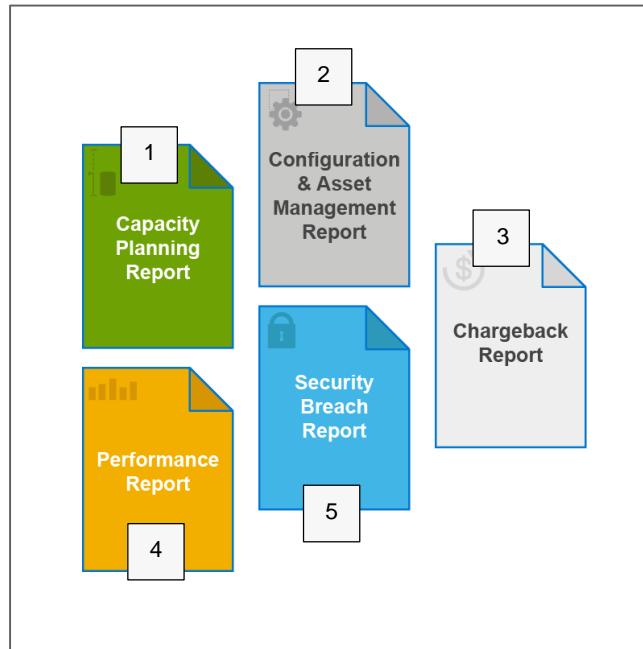


- Failure of power for storage drives, memory, switches, or availability zones.
- Storage pool reaching a capacity threshold.
- Replication operation breaching a protection policy.
- Soft media error on storage drives.

Type of Alert	Description	Example
<b>Information</b>	<ul style="list-style-type: none"> <li>• Provide useful information</li> <li>• Does not require administrator intervention</li> </ul>	<ul style="list-style-type: none"> <li>• Creation of zone or VSAN</li> <li>• Creation of a storage pool</li> </ul>
<b>Warning</b>	<ul style="list-style-type: none"> <li>• Require administrative attention</li> </ul>	<ul style="list-style-type: none"> <li>• File system is becoming full</li> <li>• Soft media errors</li> </ul>
<b>Fatal</b>	<ul style="list-style-type: none"> <li>• Require immediate attention</li> </ul>	<ul style="list-style-type: none"> <li>• Orchestration failure</li> <li>• Data migration failure</li> </ul>

## Reporting

**Reporting** on a storage infrastructure involves gathering information from various components and operations management processes. The gathered information is compiled to generate reports for trend analysis, capacity planning, configuration changes, deduplication ratio, chargeback, performance, and security breaches.



**1:** Capacity planning reports contain current and historic information about the utilization of storage, file systems, ports, etc.

**2:** Configuration and asset management reports include details about the allocation of storage, local or remote replicas, network topology, and unprotected systems. This report also lists all the equipment, with details, such as their purchase date, license, lease status, and maintenance records.

**3:** The ability to measure storage resource consumption per business unit or user group and charge them back accordingly.

To perform chargeback, the storage usage data is collected by a billing system that generates chargeback report for each business unit or user group. The billing system is responsible for accurate measurement of the number of units of storage used and reports cost/charge for the consumed units.

**4:** Performance reports provide current and historical information about the performance of various IT components and operations including success rate, failed backup and recovery operations, and compliance with agreed service levels.

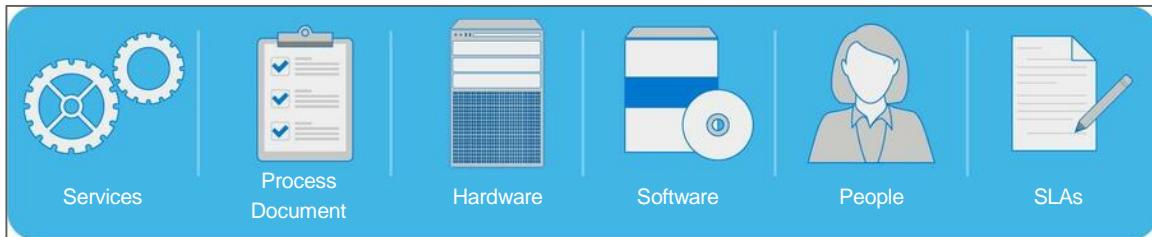
**5:** Security breach reports provide details on the security violations, duration of breach and its impact.

## Operations Management Processes

Some of the main processes of operation management include:

### Configuration Management

**Configuration management** is responsible for maintaining information about configuration items (CIs). CIs include components such as:



The information about CIs include their attributes, used and available capacity, history of issues, and inter-relationships.

### Change Management

**Change Management** standardizes change-related procedures in a data protection environment for prompt handling of all changes with minimal impact on data protection operations and service quality.

Examples of changes include:

- Introduction of a new data replication service.
- Replacing an archive storage system.
- Expansion of a storage pool.
- Upgrade of a backup application.
- Change in process or procedural documentation.



## Capacity Management

**Capacity Management** ensures that the data protection environment is able to meet the required capacity demands for protection operations and services in a cost effective and timely manner.

Examples of capacity management activities include:

- Adding new nodes to a scale-out NAS cluster or an OSD.
- Expanding a storage pool and setting a utilization threshold.
- Forecasting the usage of storage media.
- Removing unused resources from a service and reassigning those to another.



## Performance Management

**Performance management** ensures the optimal operational efficiency of all infrastructure components so that data protection operations and services can meet or exceed the required performance level.

Management tools also proactively alert administrators about potential performance issues and may prescribe a course of action to improve a situation.

Examples of performance management activities include:

- Adjusting conflicting backup schedules.



## Operations Management

- Fine-tuning file system configuration.
- Adding new VMs or allocating more resources to the existing VMs.
- Adding new ISLs and aggregating links to eliminate bottleneck.
- Adding new nodes to a protection storage.
- Changing storage tiering and cache configuration.

## Availability Management

**Availability Management** ensures that the availability requirements of data protection operations and services are consistently met.

Examples of availability management activities include:

- Deploying redundant, fault-tolerant, and hot-swappable components.
- Implementing compute cluster, VM live shadow copy, and multipathing solutions.



## Incident Management

Incident Management<sup>97</sup> is responsible for detecting and recording all incidents in a data protection environment. It investigates the incidents and provides appropriate solutions to resolve them.

The following table illustrates an example of an incident that was detected by the Incident Management tool:

---

<sup>97</sup> An incident is an unplanned event such as a switch failure, security attack, or replication software error that may cause an interruption to the protection operations and services, or degrade their quality.

## Problem Management

**Problem management** prevents incidents that share common symptoms or root causes from reoccurring, and minimizes the adverse impact of incidents that cannot be prevented. Problem management:

- Reviews incident history to detect problems in a data protection environment.
- Identifies the underlying root cause that creates a problem.
- Uses integrated incident and problem management tools to mark specific incidents as problem and perform root cause analysis.
- Provides most appropriate solution or preventive remediation for problems.
- Analyzes and solves errors proactively before they become an incident/problem.



## Security Management

**Security management** prevents occurrence of security-related incidents or activities. These incidents adversely affect the confidentiality, integrity, and availability of organizations' data. Security management ensures the regulatory or compliance requirements for data protection of organizations are met for protecting data at reasonable costs. It develops data security policies and also deploys required security architecture, processes, mechanisms, and tools.



Examples of security management activities are:

- Managing user accounts and access policies that authorize users to use a backup/replication service.
- Implementing controls at multiple levels (defense in depth) to access data and services.
- Scanning applications and databases to identify vulnerabilities.
- Configuring zoning, LUN masking, and data encryption services.

### Notes: Configuration Management

- Examples of CI attribute are the CI's name, manufacturer name, serial number, license status, version, description of modification, location, and inventory

## Operations Management

status (for example, on order, available, allocated, or retired). The inter-relationships among CIs in a data center environment commonly include service-to-user, virtual storage pool-to-service, virtual storage system-to-virtual storage pool, physical storage system-to-virtual storage system, and data center-to geographic location.

- All information about CIs is usually collected and stored by the discovery tools in a single database or in multiple autonomous databases mapped into a federated database called a configuration management system (CMS)<sup>98</sup>. Discovery tools also update the CMS when new CIs are deployed or when attributes of CIs change.

### Notes: Change Management

- Change management typically uses an orchestrated approval process that helps making decision on changes in an agile manner. Through an orchestration workflow, the change management receives and processes the requests for changes.
- Changes that are at low risk, routine, and compliant to predefined change policies go through the change management process only once to determine that they can be exempted from change management review thereafter.

---

<sup>98</sup> CMS provides a consolidated view of CI attributes and relationships, which is used by other management processes for their operations. For example, CMS helps the security management process to examine the deployment of a security patch on VMs, the problem management to resolve a remote replication issue, or the capacity management to identify the CIs affected on expansion of a virtual storage pool.

- These requests are typically treated as service requests and approved automatically. All other changes are presented for review to the change management team<sup>99</sup>.

### **Notes: Capacity Management**

- Capacity management determines the optimal amount of resources required to meet the needs of protection operations and services regardless of dynamic resource consumption and seasonal spikes in resource demand.
- Maximizes the utilization of available capacity and minimizes spare and stranded capacity without compromising the service levels. Capacity management team uses several methods to maximize the utilization of capacity such as data deduplication, compression, and storage tiering.
- Capacity management tools are usually capable of gathering historical information on the usage of backup/archiving servers and protection storage over a period of time.
  - Tools establish trends on capacity consumption and perform predictive analysis of future demand.
  - This analysis serves as input to the capacity planning activities and enables the procurement and provisioning of additional capacity in the most cost effective and least disruptive manner.

### **Notes: Availability Management**

---

<sup>99</sup> The change management team assesses the potential risks of the changes, prioritizes, and makes a decision on the requested changes.

## Operations Management

Availability management is responsible for establishing a proper guideline based on the defined availability levels of data protection operations and services. The guideline includes the procedures and technical features required to meet or exceed both the current and the future data availability needs at a justifiable cost.

Availability management team:

- Identifies all availability-related issues in a data protection environment and areas where availability must be improved.
- Monitors whether the availability of protection components and services is maintained within acceptable and agreed levels.

The monitoring tools also help the administrators to identify the gap between the required availability and the achieved availability.

- The administrators can quickly identify errors or faults in the components that may cause data unavailability in future.
- Based on the data availability requirements and areas found for improvement, the availability management team may propose and architect new data protection and availability solutions or changes in the existing solutions.

For example, the availability management team may propose an NDMP backup solution to support a data protection service or any critical business function that requires high availability. The team may propose both component-level and site-level redundancy. This is generally accomplished by deploying two or more network adapters per backup component, multi-pathing software, and compute clustering. The backup components must be connected to each other using redundant switches and/or network. The switches must have built-in redundancy and hot-swappable components. The VMs hosting backup applications must be protected from hardware failure/unavailability through VM live shadow copy mechanisms. The backup storage system should also have built-in redundancy for various components and should support local and remote backup.

## Knowledge Check

## Knowledge Check

### Knowledge Check

1. What information does infrastructure discovery identify? Select all that apply.
  - a. Configuration and connectivity
  - b. Capacity
  - c. Physical-to-virtual dependencies
  - d. Virtual-to-virtual dependencies

## Knowledge Check

2. What is a purpose of a chargeback report?
  - a. Reports resource consumption per business unit
  - b. Reports charges for SLA breach
  - c. Reports investment in managing infrastructure
  - d. Reports cost of decommissioning infrastructure components

## Knowledge Check

### Knowledge Check

3. Match the following management processes with their descriptions:

A.2. Problem management	<u>B</u>	B. Determines the optimal amount of resources required to meet the needs of IT operations.
B.1. Capacity management	<u>A</u>	A. Prevents incidents that share common symptoms or root causes from reoccurring.
C.4. Availability management	<u>D</u>	D. Makes a decision to approve or reject the request for creating a new IT service.
D.3. Change management	<u>C</u>	C. Ensures that the fault tolerance requirements of IT services are consistently met.

## Concepts in Practice

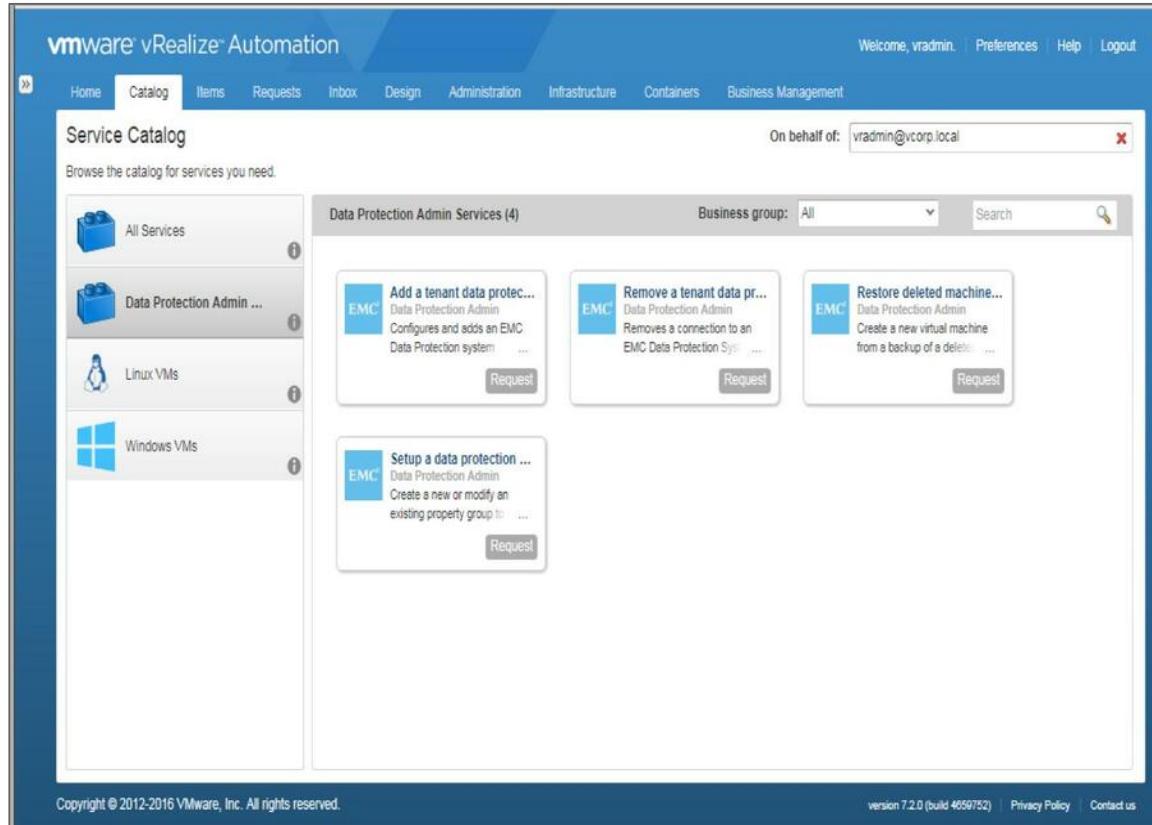
## Concepts in Practice

### VMware vRealize Suite

VMware vRealize® Suite is a purpose-built management solution for the heterogeneous data center and the hybrid cloud. It delivers and manages infrastructure and applications to increase the business agility while maintaining IT control. It provides the most comprehensive management stack for private and public clouds, multiple hypervisors, and physical infrastructure.

vRealize suite capabilities:

- Intelligent operations management to proactively addresses health, performance, and capacity management of IT services across heterogeneous and hybrid cloud environments to improve IT service performance and availability.
- Automated IT and IaaS automates the delivery and ongoing management of IT infrastructure to reduce response time to requests for IT resources and to improve the ongoing management of provisioned resources.
- DevOps-ready IT helps organization to build a cloud solution for development teams that can deliver a complete application stack.



VMWare vRealize Automation dashboard (click image to enlarge)

## Dell EMC OpenManage Enterprise

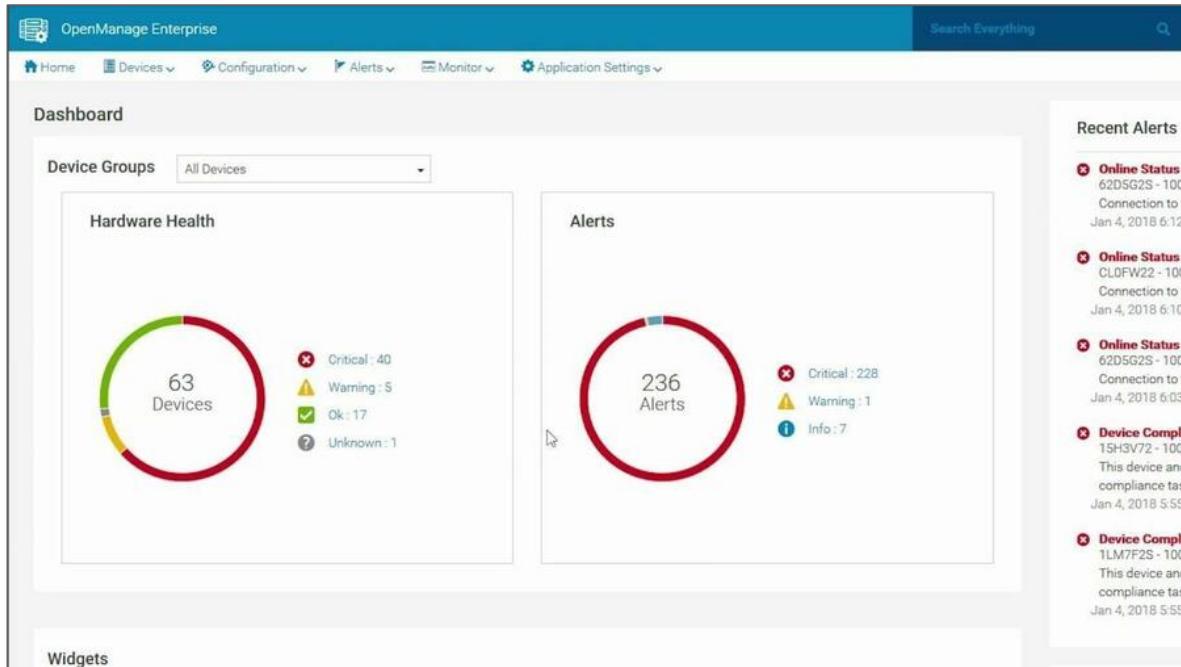
OpenManage Enterprise is a systems management and monitoring web application delivered as a virtual appliance. It provides a comprehensive view of the Dell EMC servers, storage, and network switches on the enterprise network.

With OpenManage Enterprise, a web-based one-to-many systems management application, users can:

- Discover devices in a data center environment.
- View hardware inventory and monitor health of devices.
- View and manage alerts received by the appliance and configure alert policies.
- Monitor and manage firmware / drive versions and updates.
- Manage configuration settings across devices using configuration templates.
- Detect and remediate configuration deviations across devices using configuration baselines.

## Concepts in Practice

- Retrieve and monitor warranty information for devices.
- Create and manage OpenManage Enterprise users.

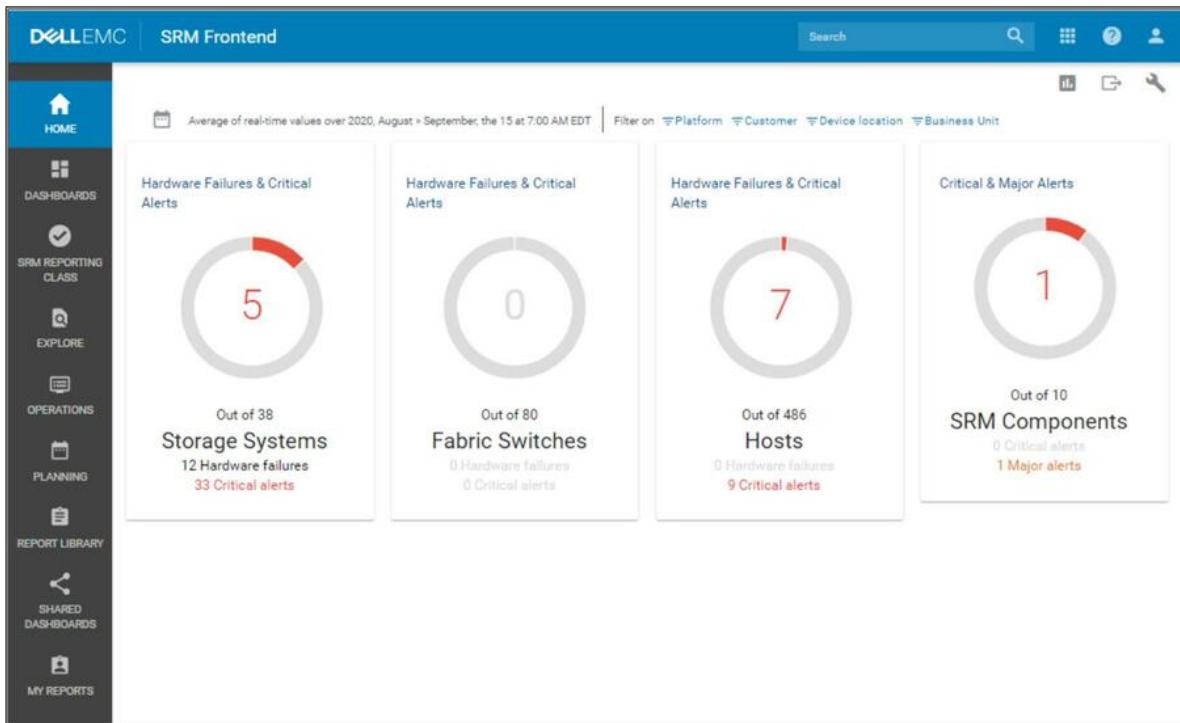


OpenManage Enterprise frontend (click image to enlarge)

## Dell EMC SRM

Storage Resource Manager (SRM) is a comprehensive monitoring and reporting solution that helps IT visualize, analyze and optimize today's storage infrastructure while providing a management framework that supports investments in on-premises and cloud storage infrastructure. SRM:

- Combines storage capacity planning and chargeback reporting for Dell EMC and multivendor storage environments.
- Supports end-to-end data path visualization for performance analysis and workload balancing.
- Provides custom, multitenant, multi-site, dashboards, and reports.
- Helps in configuration change planning and compliance monitoring to validate design best practices and the Dell EMC Support Matrix.
- Helps organizations optimize capacity and improve productivity to get the most out of their investments in block, file and object storage.



Dell EMC storage resource manager (SRM) frontend (click image to enlarge)

## Dell EMC Service Assurance Suite

Dell EMC Service Assurance Suite offers a combination of management tools including server, client and, automatic tools, to perform IT operations in a software-defined data center. Service assurance suite:

- Discovers infrastructure components and details information about each one, including configuration and inter-relationship among components.
- Detects and correlates events related to availability, performance, and configuration status of infrastructure components.
- Helps administrators to proactively resolve issues before they impact the services levels.

## Dell EMC CloudIQ

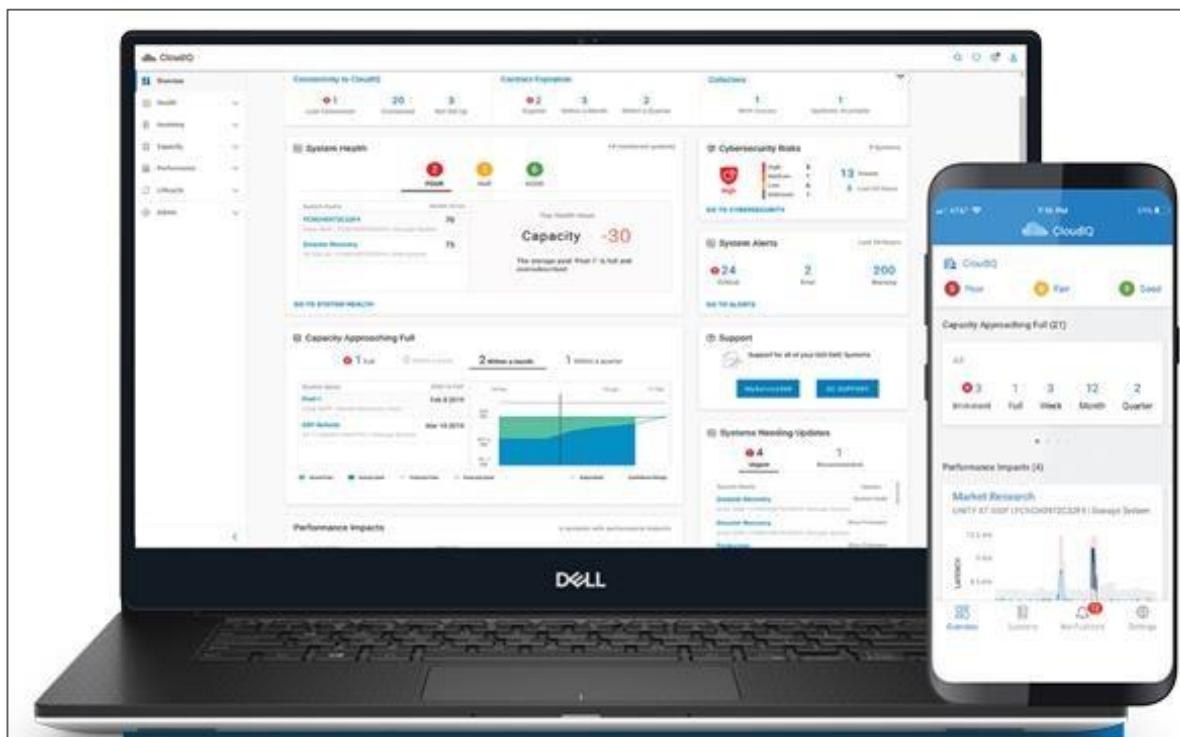
CloudIQ is the cloud-based proactive monitoring and predictive analytics application for the Dell EMC infrastructure product portfolio. It combines the human intelligence of expert engineering and the machine intelligence of AI/ML to provide

## Concepts in Practice

organization with the insight to more efficiently and proactively manage their IT infrastructure to meet business demand.

The CloudIQ portal displays your Dell EMC infrastructure systems in one view to simplify monitoring across your data center, edge and co-location sites as well as data protection in public clouds. With CloudIQ, you can easily assure that critical business workloads get the capacity and performance they need, spend less time monitoring and troubleshooting infrastructure, and spend more time innovating and focusing on projects that add new value to the organizations.

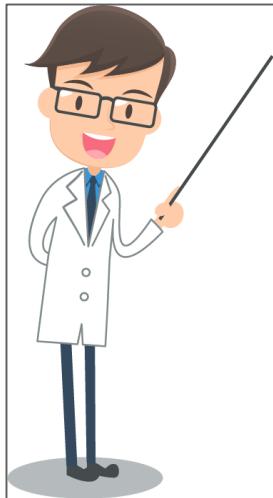
In addition to monitoring APEX Data Storage Services, CloudIQ reaches beyond on-premises data centers and edge locations to proactively monitor and predictively analyze your public cloud data protection deployments.



*CloudIQ dashboard (click image to enlarge)*

## Exercise - Storage Infrastructure Management

## Exercise: Storage Infrastructure Management



### Scenario

An organization maintaining multiple data centers provide data protection services to its customers. The details are as follows:

- Protection services cover both at local site as well as at remote site protection for disaster recovery.
  - The enterprise allows all its customer's data to be stored, protected, and accessed from worldwide location.
- 
- It has virtualized compute, network, and storage components and deployed various backup, replication, and archiving solutions.
  - It provides automated reports that are generated by monitoring and reporting tools.
  - The management operations in the data center are mostly manual.

### Challenges

- Difficulty in locating and resolving errors in infrastructure components and data protection operations.
- Difficulty in allocating resources to meet dynamic resource consumption and seasonal spikes in resource demand.
- Occasionally, the performance of replication operation gets degraded.
- Difficulty in creating the inventory of various infrastructure components including their configuration, connectivity, functions, and performance.

### Requirements

- Need to ensure adequate availability of IT resources to provide data protection services.
- Need to gather and maintain information about all the infrastructure components in a centralized database.

## Exercise - Storage Infrastructure Management

- Administrators should get proactive alerts about potential performance issues on data protection operations.
- Need to reduce manual errors and administration cost related to common, repetitive management tasks.
- Planning to deploy a new multi-site data protection service. It needs to implement a management process for architecting the new multi-site data protection solution.

### Deliverables

- Propose a solution that will address the organization's challenges and requirements.

### Solutions

- Implement a capacity management process that will help in planning for current and future resource requirements. This may include dynamic resource consumption and seasonal spikes in resource demand.
- Deploy discovery tool that gathers and stores data in a configuration management system.
- Deploy performance management tool that can proactively alert administrators about potential performance issues.
- Orchestrate management operations that are common and repetitive to reduce manual errors and administration cost.
- Implement an availability management process that will help in architecting the new multi-site data protection solution.

# Summary

## Summary

Upon successful completion of this course, participants should be able to:

- Describe business drivers of digital transformation.
- Describe modern data center infrastructure and its elements.
- Explain intelligent storage systems and their types.
- Evaluate various storage networking technologies and their deployment.
- Describe software-defined storage and networking.
- Articulate business continuity and data protection solutions (replication, backup, and archiving).
- Describe storage infrastructure security and management processes.

## Course Assessment

## Assessment Questions

## Assessment Questions

### Question

1. Which is an example of structured data?
  - a. Data stored in a relational database table
  - b. Social media activity
  - c. Surveillance video
  - d. Real-time captured photos

## Question

2. Which cloud characteristic allows a consumer to provision computing capabilities, such as server and storage, as needed automatically without requiring human interaction?
  - a. On-demand self-service
  - b. Resource pooling
  - c. Rapid elasticity
  - d. Broad network access

## Question

3. What enables multiple operating systems to share and run concurrently on a single compute system?
  - a. Hypervisor
  - b. Container
  - c. Virtual machine
  - d. Microservices

## Question

4. What is a key function of a control plane in a Software-defined Data Center?
  - a. Resource abstraction and pooling
  - b. Virtualize containerized applications
  - c. Discovery of data management tools
  - d. Provisioning physical resources to applications

## Question

5. What is a key benefit of implementing virtual provisioning?
  - a. Reduces storage capacity requirements
  - b. Reduces the need for high cache memory requirements
  - c. Increases the performance of a compute system
  - d. Increases the performance of hard disk drives

## Question

6. Which one of the following is characteristic of RAID 6?
  - a. Uses dual distributed parity
  - b. All parity resides in a single disk
  - c. Uses mirroring and striping techniques
  - d. Requires a minimum of 2 disk drives

## Question

7. Why do organizations prefer to implement unified storage systems?
  - a. Reduces management complexity
  - b. Eliminates the need for cache memory
  - c. Reduces the cost of solid-state drives significantly
  - d. Improves the performance of the hard disk drive

## Question

8. In an FC SAN environment, which port enables the connection between two FC switches?
  - a. E\_Port
  - b. F\_Port
  - c. N\_Port
  - d. NI\_Port

## Question

9. Which SAN protocol enables interconnection of local and remote FC SANs to copy the local production block storage data to remote sites?
- a. FCIP
  - b. iSCSI
  - c. FCoE
  - d. NVMe Over FC

## Question

10. What is a key benefit of software-defined storage implementation in a data center?
- a. Provides centralized management across all physical and virtual storage environments
  - b. Provides siloed storage of physical devices across departments of an organization
  - c. Improves manual storage provisioning processes that increases the performance of an application
  - d. Supports only homogeneous storage systems, which enables organizations to save cost on their storage infrastructure

## Question

11. Which statement is true about Recovery Time Objective (RTO)?
- a. Time within which systems and applications must be recovered
  - b. Point-in-time to which data must be recovered
  - c. How many Point-in-time copies are required to avoid data loss
  - d. How many times a recovery is required within a day

## Question

12. In an asynchronous remote replication, which factor impacts the Recovery Point Objective (RPO)?
- a. Size of the buffer configured on the source storage system
  - b. Type of the replica device configured on the target storage system
  - c. Type of the source device configured on the source storage system
  - d. Size of the cache memory configured on the target storage system

## Question

13. What is true about image-based backup method?
- a. Proxy server offloads the backup processing from the VMs
  - b. Proxy server automatically detects the failure of backup device and change the target
  - c. Agent is installed on all the VMs that are backed up
  - d. Agent manages the complete image of a VM

## Question

14. Which is an open access standard which enables access to resources without providing credentials?
- a. OAuth
  - b. OpenID
  - c. Multi-factor authentication
  - d. Intrusion Detection and Prevention System

## Question

15. Which is an example of security management in a data center environment?

- a. Configures zoning, LUN masking, and data encryption services
- b. Detects and resolves soft disk errors before any data loss occurs
- c. Adds new nodes to a scale-out NAS or an OSD
- d. Expands a storage pool and setting a utilization threshold

## Course Completion



