White Paper
Intel® Atom™ Processor
Intel® Xeon Processor
Cloud-based Cold Storage

Cold Storage in the Cloud: Trends, Challenges, and Solutions

Adam Mendoza
Strategic Planner, Cloud Storage
Intel Corporation

Executive Summary

Private and public clouds often use a single high-performance storage tier for most data. As enterprises and cloud service providers (CSPs) continue to experience dramatic data growth, this single-tier strategy will lead to rapidly increasing storage costs.

Much of the growing volume of information is older, "colder" data that is infrequently accessed. There's considerable potential to reduce cloud infrastructure costs by moving this data to a lower-cost storage tier specifically designed for infrequent access to cold data.

To create cloud-based cold storage that effectively meets current and future requirements, it's important to understand the usage models that are generating cold data, the challenges associated with each usage, and technologies that can help meet these challenges.

Current usage models include backup, disaster recovery, archiving, and social media. Though each usage model has distinct characteristics, they all share requirements for adequate storage performance, availability, data integrity, and security. Additionally, compatibility with existing enterprise architecture is important for seamless access to data as well as to simplify manageability, which helps reduce total cost of ownership (TCO).[1]

Although cold data is infrequently accessed, it is still incredibly valuable. Businesses are increasingly investing in "big data" analytics to identify customer and operational trends, and to gain business insights. Cold storage must therefore provide the performance and capabilities required to enable analysis.

Although cold data is infrequently accessed, it is still incredibly valuable. Businesses are increasingly investing in "big data" analytics to identify customer and operational trends, and to gain business insights. Cold storage must therefore provide the performance and capabilities required to enable analysis.

Storage based on Intel® Atom™ processors is designed to provide cost-effective cold storage with low power consumption, together with the performance headroom and compatibility to support current and future usages in multitenant clouds.[2] For storage systems requiring higher performance, Intel® Xeon® processors are code-compatible and provide higher bandwidth and processing capabilities. This compatibility enables enterprises and cloud providers to use the same applications across different Intel processors to meet the requirements of various usage models.

Intel provides a range of hardware and software technologies designed to meet the varying cloud storage needs of different businesses. Technologies designed to protect security and privacy include McAfee Endpoint Encryption*, which provides near-native performance for disk encryption by taking advantage of Intel® Advanced Encryption Standard, New Instructions (Intel® AES-NI) in Intel® processors.

Intel® Intelligent Storage Acceleration Library (Intel® ISA-L) takes advantage of other features within Intel processors to support applications designed to reduce storage cost, such as data compression and data deduplication. Intel® Cache Acceleration Software (Intel® CAS) delivers application-specific performance increases by taking advantage of Intel® solid-state drives (SSDs). In addition, enterprises and CSPs can take advantage of the Intel® Distribution for Apache Hadoop* software to accelerate performance for big data analysis.[3]

Table of Contents

The Trends Driving Cold Storage

Enterprises and cloud service providers (CSPs) continue to experience dramatic growth in the amount of data stored in private and public clouds. As a result, data storage costs are rising rapidly because a single high-performance storage tier is often used for all cloud data. However, much of the ever-increasing volume of information is "cold data"—data that is infrequently accessed. There's considerable potential to reduce cloud costs by moving this data to a lower-cost cold storage tier.

Due to the budgetary challenges of storing vast amounts of data in the cloud, cold storage is emerging as a significant trend. Some CSPs have introduced cold storage services that offer lower data storage costs and correspondingly lower performance levels. In other cases, cloud services are implementing cold storage behind the scenes; for example, they may automatically move older and less frequently accessed data to a lower-performance tier.

Because cloud-based services are evolving quickly, a key question for enterprises and CSPs is how to create a cloud-based cold storage tier that is cost-effective while meeting current and future requirements. For example, companies are gaining key business insights and identifying trends by analyzing big data (see Cold Storage and Big Data on page 6). Increasingly, the data that needs to be analyzed will include older, less frequently accessed data in cold storage. Therefore, it's important for to design cold storage that is optimized to enable data access for analysis.

COLD STORAGE REQUIREMENTS

To design cold storage that meets current and future requirements, it's important to understand the usage models that are driving growth in cold data, current and future challenges associated with each usage, and technologies that can help solve these challenges.

Cold storage usage models include backup, disaster recovery (DR), archiving, and social media applications. Though there are similarities between these models, each has distinct requirements and challenges. The requirements may be determined by corporate policy, legal compliance, governance rules, or individual needs.

Requirements such as legal e-discovery make it clear that cold data still has considerable life expectancy. Legal e-discovery requirements typically determine that archived data must be available within a specified timeframe, with evidence that the information was not tampered with. Given these requirements, the cloud provider must provide appropriate data integrity and protection as well as timely access.

Four interrelated requirements, shown in Figure 1, are relevant to most cold storage usage models. It's increasingly common to quantify and explicitly specify one or more of these requirements in cold storage service-level agreements (SLAs) between the customer and the CSP.

- **Expected storage life.** Cold storage is designed for persistent rather than transient data. This is reflected in the cold storage SLA, which is triggered by the fact that the data is considered important enough to retain and therefore requires long-term storage.
- **Access frequency.** As data ages, it tends to be less frequently accessed and therefore becomes more suited to cold storage. This may be explicitly specified in the SLA: data is moved to cold storage based on the date and time it was last accessed.
- **Access speed.** Cold storage explicitly assumes that lower performance is acceptable for older data. The SLA defines which data is needed immediately and which can wait.
- **Cost.** The benefit of cold storage is the reduced cost of storing older and less frequently accessed data. For some usage models, this overrides any other considerations. Meeting the SLA requires use of the lowest cost infrastructure. Everything else is secondary.

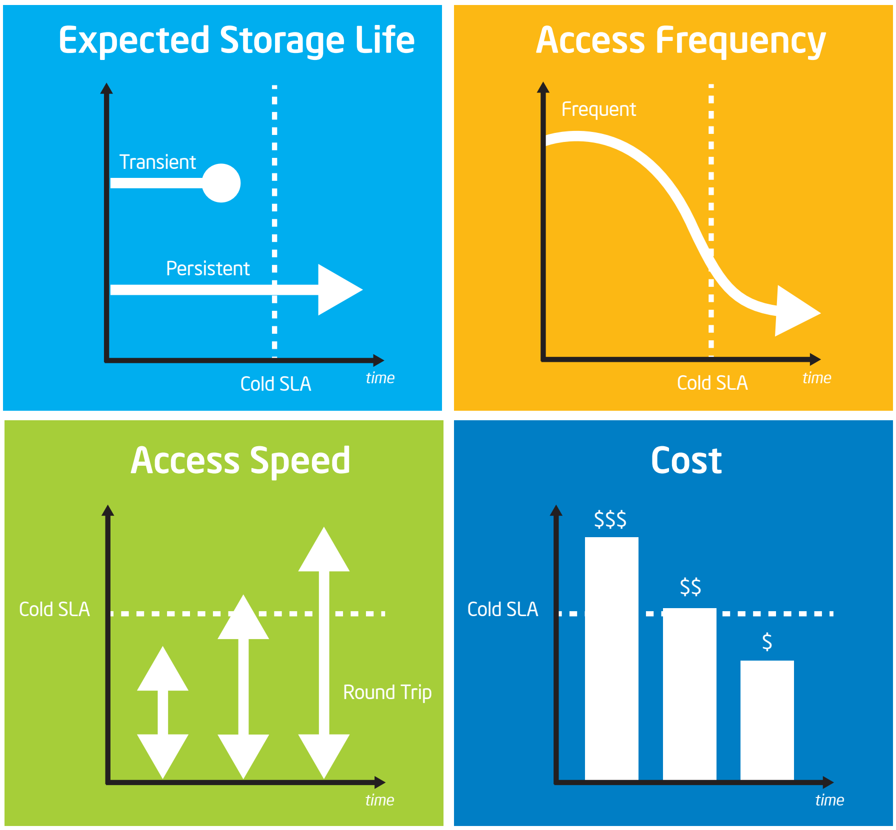


Figure 1. Cold data usage model requirements and their relationship to cloud service-level agreements (SLAs).

Cold Storage Usage Models

Cold storage usage models—backup, archiving, disaster recovery, and social media usage—share similar characteristics: infrequent data access and the need to minimize TCO per gigabyte of data stored. However, the usage models differ in the specific requirements that trigger their respective cold storage SLAs, aligning with the requirements discussed above, as shown in Figure 2. The requirements of each usage model are reflected in specific SLA provisions defining performance, availability, and data integrity. Each model is discussed in more detail below.

BACKUP

Backup is mission-critical because the data that is backed up is typically information a business needs to operate effectively; if the information cannot be recovered within a specific timeframe, the business could fail.

Cloud backup typically involves real-time, granular updates to backed-up copies of business data. For example, users may place files on an internal folder that is frequently and automatically replicated to the cloud.

Alternatively, enterprises may use a hybrid arrangement in which data is first transferred to an intermediate server within the enterprise. This server can provide various functions. It may encrypt the data before sending it to a public cloud, or it may send only a subset of critical data to reduce the costs associated with cloud data ingress and egress.

Key Challenges

Key backup challenges include enabling quick data recovery while maximizing storage efficiency.

Recovery time. The typical data recovery model is self-service. To avoid business impact, users must be able to find and recover the data they need within a specific timeframe, which is usually determined by an SLA. Key concerns are the time needed to recover data, how quickly and frequently the data is backed up (these are usually defined in SLAs as recovery time objective (RTO) and recovery point objective (RPO)), and the ability to ensure that the right copy of the data is recovered.

Meeting these requirements can be challenging; in the event of a system failure, multiple users may need to retrieve data simultaneously, creating a surge in network traffic and storage access requests. The cloud must be able to accommodate these bursts in traffic while continuing to meet the RTO defined in the SLA.

Storage efficiency. Efficiency is also a key concern; while under-provisioning storage capacity can result in performance problems, over-provisioning drives up cost.

Typical Backup SLA Objectives

Depending on the workload, backup cold storage SLAs typically define requirements in one or more of the following areas:

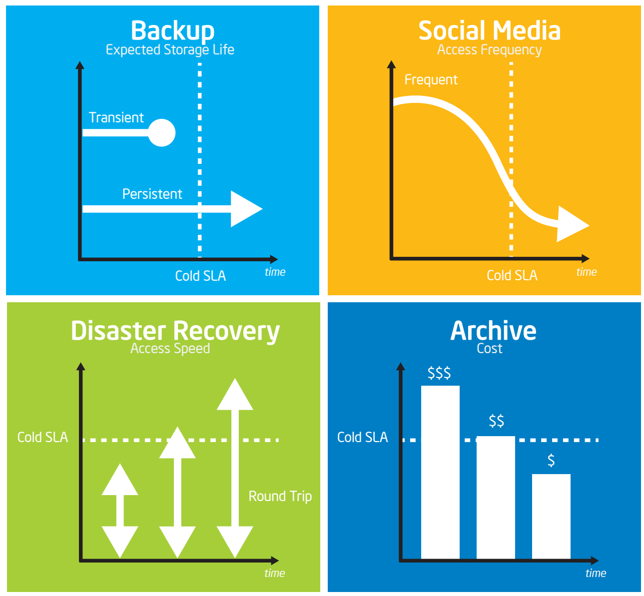
- **Performance.** RTO requirements vary depending on the workload, from less than 30 seconds to one minute.
- **Availability.** Five 9s (99.999 percent).
- **Data integrity.** The cloud provider must use specific mechanisms to protect data, such as the use of erasure codes or replication, AES 256-bit encryption, and hashing.

ARCHIVE

Archiving is business-critical rather than mission-critical. Archived information is generally important to corporate operations, customer satisfaction, or employee productivity; however, the business doesn't require immediate access to the archived data. Archiving is often required for compliance purposes, including the need to meet e-discovery requirements. As shown in Figure 2, cost is usually the overriding concern in archiving, with an expectation that costs will decrease over time. Traditionally, businesses

Backup
Used for data that is persistent and therefore requires protection. The SLA may define that data placed in a specific folder will be backed up to the cloud.

Social Media
Newly created data may be frequently accessed, but the access frequency may drop dramatically after a short time. The SLA defines that less frequently accessed data is moved to cold storage.



Disaster Recovery
The SLA defines how rapidly the entire infrastructure should become available if a disaster occurs. Warm and cold DR services may offer varying recovery times depending on how much businesses are prepared to pay.

Archive
Storage costs are a major consideration in SLAs because of the length of time that archived data must be stored. Cost may be reduced by moving data onto less expensive storage.

Figure 2. Typical cold storage usage models and their key requirements defined in service-level agreements (SLAs).

have often simply archived snapshots of data to tape, without considering how that data might subsequently be used. However, retrieving data that's been archived to tape can be a cumbersome process that can take days. This delay has become increasingly problematic as businesses rely on analysis of the data for various aspects of their operations and as data volumes increase.

Key Challenges

Archiving is a compelling cold storage usage model, but there are complex considerations related to cost, governance, and data longevity.

Managing faster, self-service access. Usages such as legal discovery require that businesses can quickly find relevant data and retrieve it within a specified period of time. The business or the cloud provider must manage the process of indexing data so that it can be quickly searched and retrieved. This can impose a significant performance overhead as the amount of stored data increases; some large clouds may include more than one billion objects. Self-service requires effective authentication between business users and external CSP systems.

Selective, policy-based archiving. Instead of archiving all documents, there are opportunities for enterprises and CSPs to reduce cost and manage compliance through selective, policy-based archiving. For example, CSPs could offer policy-based archiving services designed to meet specific legal, regulatory, and governance requirements. The system must be flexible enough to support customized retention policies, but must also incorporate immutable requirements defined by federal, state, and local governments. For example, in some countries in the European Union, it is illegal to transport some types of data across borders; this requirement must therefore be enforced by any public cloud archiving solution.

Data longevity. Many businesses may need to store data for 50 years or longer. This longevity requirement presents multiple challenges: data formats and media types become obsolete, and storage devices such as hard drives ultimately fail. This means archives must be actively managed, with the media refreshed for continued readability. Though cloud owners may be able to do this more efficiently due to economies of scale, they also face the challenge of managing this process in a multitenant environment. Constant data migration is expected to be the norm as the environment ages and components fail, resulting in the need to continually scrub and move data to meet resiliency requirements.

Typical Archive SLA Objectives

Depending on the workload, archiving cold storage SLAs typically define requirements in one or more of the following areas:

- **Performance.** Retrieval within three to five hours.
- **Availability.** Between 99 percent and 99.95 percent.
- **Data integrity.** The cloud provider must use specific mechanisms to protect data integrity, such as the use of erasure codes or replication, Intel AES-NI 256-bit encryption, and hashing.

DISASTER RECOVERY

The cloud offers great potential to reduce the cost of DR by providing multiple levels of hot, warm, and cold DR services matched to specific business needs. This provides businesses with greater flexibility to prioritize data and applications, and select the most cost-effective combination of cloud services.

For a business's most critical applications, hot standby DR services provide dedicated standby infrastructure and data in the cloud. This dedicated infrastructure means that the business can immediately switch to the cloud if a disaster occurs. Warm and cold DR services may offer varying recovery times depending on how much businesses are prepared to pay.

Cold storage services also offer the opportunity to reduce cost and complexity by eliminating some processes that businesses have traditionally used to protect against disasters. For example, if a business is using cloud backup, it may be able to eliminate the practice of backing up data to tape onsite, then moving the tape to an offsite facility for use in the event of a disaster.

Key Challenges

Key concerns for users and cloud providers are the time required to restore data and applications after a failure.

Rebuilding data files. Businesses need to know how quickly they can get their data back.

Restoring applications. Businesses need to know how quickly business-critical applications will be up and running after a failure.

When a disaster affects a business's data center or other facility, the cloud will typically experience a retrieval storm as all users of the company's applications start accessing the systems in the cloud. This may also happen if the CSP is servicing multiple tenants residing in the same region. While hot DR services typically provision sufficient dedicated infrastructure for these situations, warm and cold DR services must be able to meet demand bursts with shared cloud infrastructure.

Typical Disaster Recovery SLA Objectives

Depending on the workload, DR cold storage SLAs typically define requirements in one or more of the following areas:

- **Performance.** Recovery time from three hours to three days, with limited or no loss of transactions.
- **Availability.** 100 percent once applications and data have been recovered.
- **Data integrity.** The cloud provider must use specific mechanisms to protect data, such as the use of erasure codes or replication, AES 256-bit encryption, and hashing.

SOCIAL MEDIA

Consumer social-media companies have observed that older data tends to be less frequently accessed. For example, newly posted photos tend be viewed much more frequently than older ones, so the majority of traffic is directed to a relatively small proportion of the vast number of photos stored in the cloud. As businesses adopt social media applications, they are likely to experience a similar pattern of access. Therefore, social media data may be moved to lower-cost cold storage when access frequency drops below a specific level, as was shown in Figure 2. Users may intuitively understand, and therefore accept, that it takes slightly longer to access a photo, video, or blog post that's several days, months, or even years old.

Key Challenges

Key concerns include privacy, security, and storage efficiency.

Privacy and security. Companies and the CSPs they use to provide social-media services must adequately protect data and show that they comply with all relevant regulations.

Storage efficiency. Unstructured data, such as photos and videos, can consume vast amounts of storage capacity and is growing at a faster rate than any other type of data. Over-provisioning can therefore be extremely expensive.

Consumer social-media companies have observed that older data tends to be less frequently accessed. For example, newly posted photos tend be viewed much more frequently than older ones, so the majority of traffic is directed to a relatively small proportion of the vast number of photos stored in the cloud. As businesses adopt social media applications, they are likely to experience a similar pattern of access. Therefore, social media data may be moved to lower-cost cold storage when access frequency drops below a specific level.

Typical Social Media SLA Objectives

Depending on the workload, social media cold storage SLAs typically define requirements in one or more of the following areas:

- **Performance.** Recovery time greater than three seconds.
- **Availability.** Typically 99.95 percent or better.
- **Data integrity.** The cloud provider must use specific mechanisms to protect data, such as the use of erasure codes or replication, Intel AES-NI 256-bit encryption, and hashing.

Cold Storage and Big Data

Big data analysis is a fast-growing trend that enables companies to obtain business insights by analyzing huge volumes of information from a variety of sources. Though a range of business intelligence tools have been used in the past, new technology such as Apache Hadoop* enables big data analysis to be performed in a highly cost-effective way using open-source technology running on Intel®-based platforms. The technology can be used to analyze information including data gathered from website visits, customer buying behavior for specific demographics, and IT event and application logs.

Big data analytics can be applied to multiple cold storage usages, including:

Backup. Typical backup tools do not differentiate between information that may be considered important, is most frequently accessed, and therefore should be kept locally as opposed to off-site. Analytics can be used to sift through large volumes of data to determine which items have changed and therefore need to be backed up. This can help save time while reducing consumption of processing capacity and network bandwidth.

Archive. Long-term retention of corporate information provides an opportunity to understand trends that may not be apparent when viewed across shorter periods of one or two years. Analyzing data such as changes in the buying habits of specific customer demographics over time can help companies optimize their investments as they seek to retain customers and design new products.

Social media. Bursts of social media activity can be early indicators of trends that represent global marketing opportunities. Capturing, analyzing, and correlating "viral" social media trends can help companies determine how to allocate marketing budgets.

Disaster recovery. Effective disaster recovery in the cloud depends on the reliability of the cloud provider's infrastructure. Detailed analysis of providers' experience, utilization, and past history may provide useful statistics about the reliability of services.

Implementing Cloud Cold Storage Using Intel® Processors

Storage based on Intel processors and technologies includes a broad range of capabilities that are designed to meet the challenges of each of the cold storage usage models—backup, archiving, disaster recovery, and social media.

Depending on the usage model, cold storage must meet a range of requirements in addition to providing capacity at low cost. These requirements include performance, availability, data integrity, compatibility, and manageability. Analytics should be considered a primary cold-storage workload, enabling businesses to derive value from older data.

Intel processors include features designed to meet cold storage requirements, supporting key functions such as encryption, RAID, erasure codes, hashing, and compression. The value of these functions for cold storage is described further below. Applications can take advantage of these features, depending on the processor, using the Intel ISA-L, which includes optimized algorithms that can help accelerate many of these functions.

PERFORMANCE AND COST CONSIDERATIONS

Though cost is the primary business driver for cold storage, performance is still important. To meet SLAs using shared cloud infrastructure, cloud owners must include enough performance headroom to handle requests from multiple users and applications during demand peaks. Storage based on industry-standard servers with Intel Atom processors is designed to reduce cost while offering the performance headroom required for current and future uses.

Using Intel ISA-L, applications can take advantage of features within Intel processors to help accelerate functions that increase storage efficiency, such as thin provisioning, data compression, and data deduplication. For example, deduplication uses hashing extensively when comparing files in order to identify duplicates that can be removed; data egress may require intense use of compression functions to "rehydrate" a previously compressed large data set.

In addition, Intel CAS delivers application-specific performance increases on physical and virtual platforms, taking advantage of Intel SSDs.[4] This increased performance lets systems support more concurrent users and more virtual machines (VMs) running I/O-intensive applications. To optimize performance, Intel CAS policy management allows fine-grained control over data caching—at the level of specific applications, files, and database tables.

AVAILABILITY AND MANAGEABILITY

Storage requires significant qualification and validation for data access and data integrity. For businesses that already run their applications on Intel® architecture, a cloud based on Intel architecture helps provide full compatibility. This is important for all cold storage usage models, since businesses need to retain the ability to access data for analysis or other purposes after it has been moved to cold storage. It is a key consideration for disaster-recovery services, which must provide assurance that businesses will be able to run their applications in the cloud. As additional storage tiers are deployed in private and public clouds, using multiple architectures adds to the risk of incompatibility.

Using a standard architecture for all storage tiers also simplifies management of the environment, helping to reduce TCO. Many software suppliers have stringent compatibility requirements that the infrastructure must meet. With multiple architectures, there may also be requirements to convert or recompile applications and use multiple sets of management processes and tools.

ERASURE CODE

Today, many CSPs and enterprises use triple replication to safeguard data against loss. Erasure code, supported by features within Intel processors, is a highly efficient alternative designed to significantly reduce the storage capacity required. A more distributed and scalable approach than traditional RAID, erasure code allows greater tolerance of disk failures and faster drive rebuild times. Data can be distributed across a data center and even between data centers, supporting disaster recovery.

DATA INTEGRITY AND SECURITY

All cold storage usage models involve the storage of information that's often personal, confidential, or sensitive in other ways. Therefore, clouds must use mechanisms to protect this data in transit and at rest.

Intel provides a range of technologies designed to protect security and privacy. These include Intel AES-NI, a set of instructions within Intel processors and available through Intel ISA-L, that provide hardware support for encryption. Applications that take advantage of Intel AES-NI include McAfee Endpoint Encryption, which provides near-native performance for disk encryption.[5] Other Intel ISA-L functions are designed to accelerate hashing and checksum features used to help assure data integrity and support authentication.

Intel processors also include capabilities designed to help secure virtualized cloud environments remain, such as Intel® Virtualization Technology (Intel® VT) virtual machine isolation and Intel® Trusted Execution Technology (Intel® TXT).

ANALYTICS

Although cold data is infrequently accessed, it is still incredibly valuable. Businesses are increasingly investing in big data analytics to identify customer and operational trends, and gain business insights. Even if businesses are not analyzing historical data today, they may well need to do so in the future to remain competitive. It is therefore essential to consider performance headroom and other capabilities required for big-data analysis when defining storage requirements. With storage based on Intel processors, enterprises can take advantage of Intel® Distribution for Apache Hadoop* software. This software platform provides distributed processing and data management for enterprise applications that analyze massive amounts of diverse data.

Conclusion

Cloud-based cold storage offers the potential for compelling financial benefits; however, there's more to cold storage than simply reducing costs. For all usage models, cold storage must meet a broad range of requirements in areas including performance, accessibility, data integrity, security, and compatibility.

Big data analysis makes it clear that cold data is not as cold as it may seem. Analysis can extract compelling business insights from historical and other infrequently accessed data, helping companies remain competitive by optimizing key business functions such as customer retention and new product development. Therefore, analysis should be considered a primary cold-storage workload; it is essential that cold storage include adequate performance headroom and other capabilities required to enable big-data analytics. Intel provides a broad range of technologies designed to enable and accelerate big-data analysis, including Intel Distribution for Apache Hadoop software.

Intel processors and acceleration software are designed to enable highly cost-efficient cold storage with low power consumption, enhance security and privacy, and provide the performance headroom to meet current and future requirements in multi-tenant cloud environments.

For more information about Intel®-based storage solutions, visit **www.intel.com/go/storage**.

Acronyms and Terms

CSP	cloud service provider
DR	disaster recovery
Intel AES-NI	Intel® Advanced Encryption Standard, New Instructions
Intel CAS	Intel® Cache Acceleration Software
Intel ISA-L	Intel® Intelligent Storage Acceleration Library
Intel TXT	Intel® Trusted Execution Technology
Intel VT	Intel® Virtualization Technology
RPO	recovery point objective The maximum acceptable time period prior to a failure or disaster during which changes to data may be lost as a consequence of recovery. Data changes preceding the failure or disaster by at least this time period are preserved by recovery. Zero is a valid value and is equivalent to a "zero data loss" requirement.[6]
RTO	recovery time objective The maximum acceptable time period required to bring one or more applications and associated data back from an outage to a correct operational state.[7]
SLA	service-level agreement
SSD	solid-state drive
TCO	total cost of ownership
VM	virtual machine

1 The TCO or other cost reduction scenarios described in this document are intended to enable you to get a better understanding of how the purchase of a given Intel product, combined with a number of situation-specific variables, might affect your future cost and savings. Circumstances will vary, and there may be unaccounted-for costs related to the use and deployment of a given product. Nothing in this document should be interpreted as either a promise of or contract for a given level of costs.

2 http://newsroom.intel.com/community/intel_newsroom/blog/2013/09/04/intel-unveils-new-technologies-for-efficient-cloud-datacenters

3 Intel® Distribution for Apache Hadoop* software http://hadoop.intel.com/products/distribution

4 www.intel.com/content/www/us/en/software/intel-cache-acceleration-software-product-brief.html

5 www.mcafee.com/us/products/endpoint-encryption.aspx

6 www.snia.org/education/dictionary/r

7 Ibid.

Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules, and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit www.intel.com/technology/security.

(Intel® VT) Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance, or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.

Printed in USA 1013/AM/VF/PDF Please Recycle 329256-001US