HITACHI
Inspire the Next

WHITE PAPER

The Path to 10 Nines Availability With Hitachi Content Platform (HCP)

By Hitachi Vantara

October 2017

Contents

Executive Summary

Availability of cloud storage systems consists of accessibility (system uptime) and durability (intact data), both of which are measured as the expected percentage of availability per year. Values are expressed as the number of nines following the decimal separator (for example, “three nines” = 0.999 = 99.9% availability). A globally distributed Hitachi Content Platform (HCP) using HCP S series storage provides 10 nines of accessibility with 15 nines of durability, which is equivalent to three milliseconds of annual downtime and one lost object in 100 trillion years per thousand objects. These levels of availability are appropriate for a backup-less cloud platform and are achieved through self-healing and self-monitoring functions that operate both locally and globally. Allowing the addition of new hardware, retiring old hardware, and upgrading software levels, without disrupting service, also eliminates planned downtime.

In the event that a site or HCP system is unavailable, users and applications can transparently access another HCP system at another site, ensuring continuity of service with 10 nines accessibility. HCP can rebuild content using fragments dispersed across clusters, an approach which consumes up to 40% less storage than mirroring the entire set of data. An HCP system includes at least four access nodes and can continue full operation despite the failure of a node, resulting in five nines accessibility at the individual cluster level. An access node is the server that serves as a building block for an HCP cluster, and includes multiple redundant components and 99% node-level accessibility.

Each object stored on an HCP S series storage node is dispersed across drives, and each fragment can survive the simultaneous loss of six drives, providing a durability of 15 nines. Besides orders of magnitude higher resiliency than RAID, the HCP S systems offer Reed-Solomon Erasure Coding, which delivers higher capacity efficiency than RAID-6 and RAID-5. HCP’s data-protection-level policy ensures a number of copies of each object are maintained and self-heals when a copy is unavailable. When data is stored on HCP’s access nodes, it leverages both the data protection level and underlying RAID-6 to provide at least 13 nines durability. Background services periodically run on access nodes to ensure the integrity of content and metadata.

Introduction

IT is moving from rigid system architectures to cloud infrastructure platforms for their advantages in flexibility, cost and service orientation. While effects of downtime in a traditional architecture are confined to relatively few systems, when the cloud platform itself is unavailable, the impact is magnified: It can take all mission-critical services (and noncritical services) offline. So IT is obliged to deliver higher levels of availability for the cloud platform than it has with traditional systems.

Hitachi Content Platform (HCP) is an object-based storage system designed to be the core for a large-scale, private or hybrid cloud platform. It is a self-monitoring, self-healing system that is able to deliver extremely high levels of service availability without the overhead of traditional architectures, such as backup.

This white paper explains the configurations and mechanisms that HCP uses to achieve high availability. Each chapter builds upon the capabilities explained in the prior chapter until reaching 99.9999999% ("10 nines") accessibility and 99.9999999999999% ("15 nines") durability. The math and methodology can be found in the callout box in each section. But before we get into the technology, the next section provides clarity on what exactly we're measuring.

Defining Availability, Accessibility and Durability

> *"Availability = accessibility (can you get to your application and data) + durability (is the data intact and consistent)"*[1]

In the context of cloud storage services, availability means system accessibility with storage durability. Accessibility means systems are running and you can effectively communicate with them, and durability means the data bits are unperturbed. Durability of storage is pointless if you can't access the systems that provide the data, and system accessibility is worthless if the underlying data is corrupt or lost: You need both accessibility and durability for a service to be "available."

A service's availability level is measured by the time it is available divided by total time. This is commonly discussed in terms of "nines" and the amount of time the service is not available ("downtime"), as shown in Table 1.

Table 1. Nines and Availability Levels

Number of Nines	Availability Level	Downtime per Year (approx.)
1	90%	5 weeks
2	99%	4 days
3	99.9%	9 hours
4	99.99%	53 minutes
5	99.999%	5 minutes
6	99.9999%	32 seconds
7	99.99999%	3 seconds
8	99.999999%	316 milliseconds
9	99.9999999%	32 milliseconds
10	99.99999999%	3 milliseconds

Background Reading

This paper assumes a basic understanding of HCP components, which can be gained by reading the Hitachi Content Platform Architecture Fundamentals white paper. It is also worth noting that malicious activities can result in downtime, which can be mitigated through security measures. The Hitachi Content Platform Security white paper thoroughly addresses the security capabilities, which are beyond the scope of this paper.

Planned downtime occurs when a system must be unavailable during upgrade, maintenance or migration. Unplanned downtime occurs when there is failure of a critical part, system or area without having recovery mechanisms that continue to service requests.

[1]Schulz, G. (2017). *Software-Defined Data Infrastructure Essentials.* Boca Raton, FL: Auerbach Publications .

HCP's nondisruptive upgrades and automated technology refresh eliminate the need for planned downtime and HCP has self-healing and recovery mechanisms built into every layer to prevent unplanned downtime. But just like every system out there, HCPs may face circumstances when availability can be briefly interrupted. For example, after a failover, applications may wait for protocol timeouts or for data that was queued to be replicated, or the system intentionally could be taken offline for performance reasons. And there is some chance of a software bug that could impact availability. HCP code undergoes continuous quality improvement, so the risk decreases over time. HCP is designed to provide multiple redundancies, but not all types of errors can be accounted for in availability calculations.

Storage durability refers to the chance that data has been permanently lost. Hard drive failures and uncorrectable errors can lead to lost data, but storage systems can salvage and repair data using RAID, erasure coding, replication and other techniques. The durability of a storage system is increased when additional simultaneous difficulties do not permanently lose data. You can measure durability by the time you would expect to lose a piece of data, as shown in Table 2.

Table 2. Nines and Durability Levels

Number of Nines	Durability Level	Average Time Until One Lost Object per Thousand Objects
1	90%	4 days
2	99%	37 days
3	99.9%	1 year
4	99.99%	10 years
5	99.999%	100 years
6	99.9999%	1,000 years
7	99.99999%	10,000 years
8	99.999999%	100,000 years
9	99.9999999%	1,000,000 years (1 million)
10	99.99999999%	10,000,000 years
11	99.999999999%	100,000,000 years
12	99.9999999999%	1,000,000,000 years (1 billion)
13	99.99999999999%	10,000,000,000 years
14	99.999999999999%	100,000,000,000 years
15	99.9999999999999%	1,000,000,000,000 years (1 trillion)

(For scale: Evidence of *Homo sapiens* is 200,000 years old, life on Earth started about 4.5 billion years ago, and the universe is about 13.8 billion years old)

So let's dive into the details of accessibility and durability characteristics of the core technology, which provides…

99% (Two Nines) Availability: Single Access Node – Unsupported Configuration

A single access node is never deployed alone (the minimum configuration for HCP is four access nodes) but each access node in isolation is a "building block" that has a good availability profile.

When the access node is deployed as an appliance (for example, the HCP G10, also known as "G node," as shown in Figure 1) it is a conventional x86 server that runs a Linux-based operating system. The server has redundant Ethernet ports that connect to redundant front-end networks (and redundant back-end networks depending on configuration). The server includes dual redundant, hot-swappable power supply units. These are cabled into separate power distribution units (PDUs) connected to different power circuits. Loss of one power phase should not affect availability. Loss of a power supply should not affect availability, and the power supply can be swapped out with any downtime. The cooling for the server is provided by redundant fans.

Figure 1. Example HCP G10 configured with 10G SFP+ ports for both front- and back-end connections with an additional pair of bonded Ethernet ports.

A Hitachi Vantara analysis calculated the hardware availability of a standalone HCP G10 access node as approximately 99.84%. This is in line with expectations for industry-standard server availability.

> Server availability is calculated by multiplying the availability of each hardware component in the server. Hardware availability was calculated as $\frac{\text{MTBF}}{\text{MTBF+MTTR}}$. When a system is composed of multiple hardware components, each of which could bring down the system, you multiply the availability of each component to get the availability of the system as a whole (thus reducing the system availability level): $\text{A} = \text{A}_\text{X}\text{A}_\text{Y}$. For a component with a redundant duplicate, the combination is considered failed only when both parts fail and the combined availability is: $\text{A} = 1 - (1 - \text{A}_\text{X})^2$ where A_X is the availability of the component.

HCP provides alerting via SNMP and Hi-Track Remote Monitoring so that incipient problems can be addressed before they become serious. The baseboard management controller (BMC) in the servers also provides SNMP and IPMI monitoring of components and environmental conditions so that faults in redundant components, temperature extremes or power quality issues can be addressed in a timely manner.

A single HCP G10 node can thus survive the failure of a PDU, cooling component or network port. But other failures can make a single node unavailable, which is why HCP requires at least four access nodes.

99.9999% (Six Nines) Durability: RAID-6 on an Access Node

A single access node has protection at multiple levels to ensure the data resilience, in the software as well as the hardware safeguards.

An often-overlooked form of data durability is recovery from the accidental deletion of data. HCP also includes versioning and retention capabilities that are able to prevent object deletion and salvage accidentally deleted objects.

An HCP access node runs background services that ensure the integrity of both the data and metadata. To that end, while an object is stored, HCP also stores hash signatures based on the object, the object's system metadata, and the object's custom metadata. The **content verification** daemon periodically validates that stored objects and metadata match their hashes to detect silent data corruption and then correct it. The service will repair a corrupted object by finding a good copy, even going so far as checking other HCP clusters to which the object was replicated. (These object copies will be covered in the next chapters.) HCP also checks the hash when the object is accessed to ensure that it has not been corrupted.

Storage for a G node uses internal hard drives configured in a RAID-6, which provides protection against two disks simultaneously failing, and 99.9999% (six nines) durability. In addition, the hard drive hardware and communication protocols have various mechanisms to prevent, detect and repair data corruption.

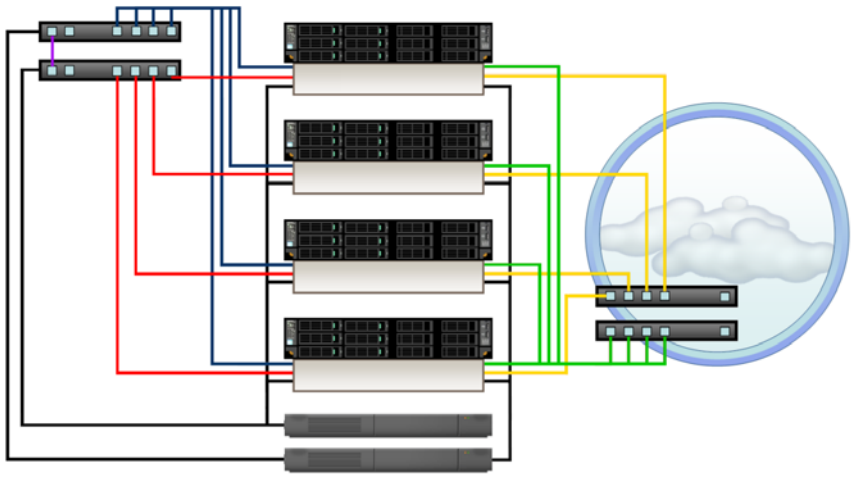
The classic approach for calculating RAID-6 durability is the Mean-Time-to-Data-Loss equation for RAID-6: $\mathrm{MTTDL} = \frac{\mathrm{MTBF}^3}{\mathrm{N}\times(\mathrm{N}-1)\times(\mathrm{N}-2)\times\mathrm{MTTR}^2}$ where N=number of disks in the RAID group. HCP access nodes use a configuration of 6 disks (4 data + 2 parity) and we'll use a typical[2] MTBF of 292,000 hours and a disk rebuild time of 16.05 hours for 4TB nearline (NL)-SAS, based on Hitachi Vantara's testing plus another 72 hours for worst-case next-business-day replacement. So this gives a mean of 3,058,425 years to data loss. It doesn't imply that a RAID-6 will survive for 3 million years, but it implies a 1 in 3 million chance of failing over one year, which is a durability of 99.9999% (6 nines).

99.999% (Five Nines) Accessibility: Four-Node, Shared Nothing Cluster

When deployed in a basic configuration (a cluster of four) the access nodes coordinate to provide a highly resilient system that satisfies the availability requirements of many IT departments. In the simplest configuration, each node manages a private pool of internal storage, which we describe as a "shared nothing" configuration.

HCP clusters employ redundant data paths as visible in Figure 2. This becomes the foundation of a layered approach to availability by clustering servers and running self-healing software on the clusters. There are dual redundant Ethernet connections from the server to the front-end network and dual redundant connections to the back-end network. Organizations are encouraged to cable these circuits to independent switches to ensure the highest accessibility in the event of a cable or switch problem. By employing two separate switches, rolling software updates can be performed on the switches without affecting accessibility. The power to each access node should come from two separate PDUs as well.

Figure 2. HCP Redundant Connections (Back-end network: Red + Blue + Purple; Front-end network: Green + Yellow; Power: Black)



Any HCP access node in the cluster is able to receive an I/O request; if the requested data is not in the node's internal storage, it forwards the request to the least-busy node that does have a copy. The access nodes are all actively working to service I/O: They are not "standby" or "passive" nodes. The best practice when configuring HCP

[2] Drives used in HCP and HCP S series are rated MTBF of 1.6M/hr. (0.63% AFR), 2.0M/hr. (0.44% AFR), or 2.5M/hr. (0.35% AFR). But real-world observations found in academic research is closer to 292,000 – not matching the rated levels.

clients is to utilize DNS (or a network load balancer) to round-robin requests across all nodes to ensure maximum accessibility rather than directing clients to a specific node.

HCP overcomes a durability limitation of using internal storage by maintaining copies of data on multiple nodes. Each namespace has a data protection level (**DPL**), which specifies how many copies of each object HCP must maintain. HCP automatically keeps each copy on different nodes, so that if one node is inaccessible the information is still accessible via another node. In a shared nothing cluster, the DPL must be two or greater, meaning there must be at least two copies of every object.

> To calculate the availability of a cluster consisting of HCP G10 nodes, we'll just consider the availability of a pair of nodes in a four-node cluster when DPL is two. Because the nodes operate as redundant the combined availability of a single HCP cluster is $1 - (1 - 99.84\%)^2 = 99.9997\%$. This is "five nines" of availability.

The access nodes coordinate via an isolated, private and back-end network, which is designed with redundancy: Each node has a bonded Ethernet port pair connected to two unstacked switches plus an inter-switch link. The back-end network can survive the failure of a switch and the system will continue to operate.

So far, we've discussed reduction of unplanned downtime, but an HCP cluster also eliminates **planned downtime**: old hardware can be retired, new hardware can be introduced, and the software version can be upgraded – all without disrupting service. The **autonomic tech refresh** feature is able to retire equipment by gradually moving data in the background to existing or new hardware and then disengaging from the old hardware.

Based on these capabilities, a HCP shared-nothing cluster can still remain accessible despite a node experiencing downtime.

99.99999999999% (13 Nines) Durability: DPL2 on RAID-6

At the HCP cluster level, the data protection scheme is robust enough that backups of an HCP cluster are unnecessary: The system has built-in data resiliency at the server, data, metadata and storage levels.

At the heart of the cluster level's durability is the DPL policy. When content is written to HCP with DPL2, HCP ensures that there are two copies of the object on different nodes before confirming the write back to the client. And HCP prohibits system changes that will reduce the number of object copies to below the required DPL. The administrator may increase DPL up to four, which increases the number of copies of data, thus increasing the durability.

If a failure causes the number of copies of an object to fall below the DPL, HCP will automatically take corrective action. For example, if a node goes offline in a DPL2 (two copies) environment, HCP realizes that the data stored on that node might be permanently gone; this violates the DPL policy because only one copy of the data may now exist. So HCP will create additional copies of the objects from the remaining copy to return to DPL2. If the node recovers, the extraneous copies will be deleted to free up space.

Using a RAID-6 configuration with a DPL2 means that there are two independent RAID-6 groups with the same data. The data loss scenario is quite extreme: One RAID group would have to have a double-disk failure and then another RAID group on another node containing the second copy would have to have a double-disk failure prior to HCP completing its self-healing. Because of the rarity of a quadruple-disk failure, the durability is 99.99999999999% (13 nines).

The HCP's data protection level effectively acts like a mirror, providing a RAID-1+6 durability level. So, we can apply the RAID-1 durability formula to the underlying RAID-6 protection. For a DPL2 the calculation to use is $\mathrm{MTTDL}_{\text{RAID-1+6}} = \frac{\mathrm{MTTDL}^2_{\text{RAID-6}}}{2\times\mathrm{MTTR}_{\text{RAID-6}}}$. The $\mathrm{MTTR}_{\text{RAID-6}}$ is how long it takes to recover from a DPL1 scenario to DPL2 scenario, typically by replicating the surviving copy of the data to another access node. The most realistic scenario is unrecoverable loss of one HCP G10 node, so we'll estimate a time of 3000 hours to self-heal the entire second copy of the affected data (14TB) to other nodes. This results in a mean of 13,656,788,116,841 (13 trillion) years to data loss, which is a durability of 99.99999999999% (13 nines). If we only considered loss of one RAID group (not a whole HCP G10 node), then there is less data to self-heal, so the recovery time ($\mathrm{MTTR}_{\text{RAID-6}}$) would be reduced, and the durability would be even higher.

The downside of mirroring the data is that double the storage capacity is consumed, which leads to a higher cost for effective capacity.

In addition to enforcing a DPL policy, HCP also enforces a metadata protection level (**MPL**), which is the number of copies of the object metadata that HCP must maintain on different nodes. Analogous to how HCP treats DPL violations, HCP will automatically take corrective action to create additional copies of metadata. Both the DPL and MPL enforcement is performed by the **protection** daemon.

The **scavenging** background process periodically verifies the integrity of the metadata. It checks the various copies of metadata to make sure they are existent, complete, valid and in sync with each other. If it finds errors, it tries to rebuild or repair the problem metadata.

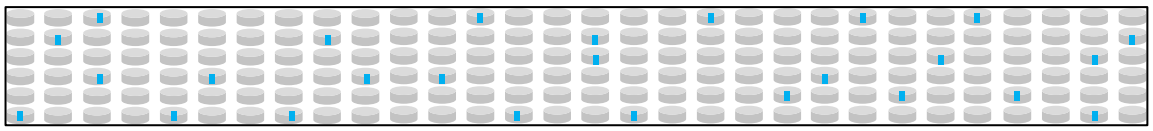
99.9999999999999% (15 Nines) Durability: HCP S Series

As a more efficient alternative to utilizing storage internal to the access nodes, HCP can use HCP S storage nodes (also known as "S series" or "S nodes") that use erasure coding for more efficient data protection. In these configurations, the access nodes only contain the HCP operating system and metadata.

Access to the S node data survives even in the event of an access node failure. S nodes are connected via the front-end network so that all access nodes are able to directly access all of the S nodes. When the access node receives an I/O request, it queries the cluster to identify where the content is stored and then it communicates with the appropriate S node.

HCP S series storage uses Reed-Solomon Erasure Coding as a more resilient and efficient protection approach than RAID-6. Disk sizes have grown larger and erasure coding can repair these larger disks much faster than RAID-6, and thus improve durability immensely. The technique divides each object into data fragments, with each fragment distributed across 26 drives (20 data and six parity). For example in an HCP S30 node with 90 drives, one data fragment might be spread across 26 drives as shown in Figure 3.

Figure 3. Fragments are distributed across drives.



Even with the simultaneous loss of six drives containing object fragments, the object is still readable. The data durability for an S node is 99.9999999999999% (15 nines).

Durability of erasure coding data can be calculated using the formula derived and defined in the white paper, "Comparing Cost and Performance of Replication and Erasure Coding": $\sum_{i=n+1}^{m+n} \binom{m+n}{i} P_L^i (1 - P_L)^{m+n-1}$, where probability of more than *n* failures in an *m+n* system when each component has probability of failure P_L, *m* is the number of data fragments, and *n* is the number of parity fragments. In an S node the *m* is 20, *n* is 6 and P_L is 0.041841%. P_L is calculated using a disk rebuild time of 120 hours and 5% hard drive AFR.

The data durability for a single S node is calculated to be 99.9999999999999% (15 nines). This means the chance of losing an object is 0.000000000000001% -- effectively nothing. For example, if you store 1,000 files in HCP you can, on average, expect to lose a single object every trillion years.

The hardware availability for standalone HCP S10 and HCP S30 storage nodes was calculated to be 99.999% (five nines) similarly to the G node calculation. This is typical for an external storage architecture that utilizes dual controllers. When storage nodes are replicated across clusters the availability for the data increases to 10 nines because the replica serves as a redundant component.

In addition to having higher durability the S node erasure coding uses less overhead capacity than RAID-6 and even RAID-5, resulting in a very cost-efficient and reliable system, as shown in Table 3.

Table 3. Durability With S Node Erasure Coding

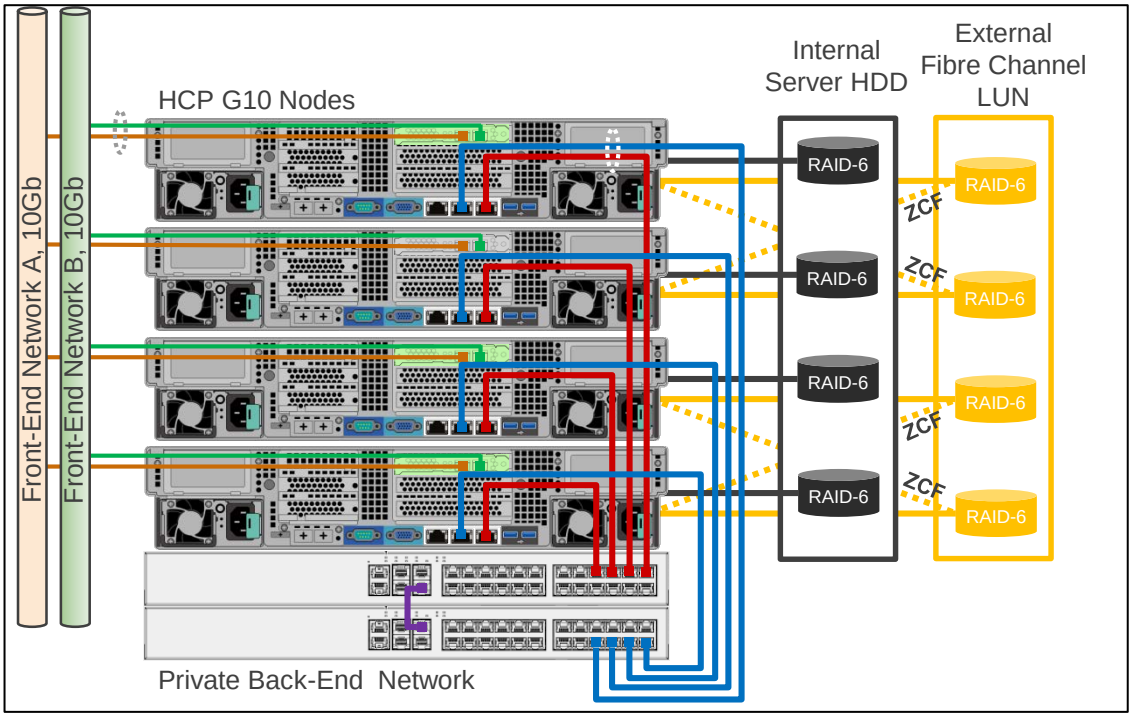
	Durability	**Usable Capacity**
RAID-5 (4+1)	99.9% (three nines)	73.0%
RAID-6 (4+2)	99.9999% (six nines)	60.8%
DPL2 on RAID-6	99.99999999999% (13 nines)	30.4%
Erasure Coding (20+6)	99.9999999999999% (15 nines)	76.9%

SAN Storage Availability and Durability

An HCP cluster can utilize SAN-attached arrays, which provide various levels of availability and durability, beyond the control or scope of HCP. Some HCP customers use DPL1 with a RAID-6 configured SAN for capacity savings while being comfortable with its availability.

In a SAN-attached configuration, access nodes are paired and given standby access to each other's LUNs on the SAN, a process called *cross-mapping,* which utilizes multipathing. In the event of an access node failure, the surviving node assumes ownership of the standby LUNs, called **zero copy failover,** thereby ensuring continuous access to the content stored on the SAN. In Figure 4, each node in a four-node HCP cluster has its own Fibre Channel LUN and also a ZCF-accessible LUN.

Figure 4. Hitachi Content Platform G10 Nodes in SAN-Attached Configuration



99.99999999% (10 Nines) Accessibility: Multisite Geo-Replicated Clusters

HCP is designed so that separate clusters can be placed in different locations for performance and availability purposes, and the clusters can coordinate access and replicate data. During normal operation accesses of objects can use the nearest replica to provide proximity-based performance. HCP's multisite clusters include resiliency to ensure the continuity of the service and data even in disaster scenarios. Replication is asynchronous to maximize performance and, therefore, may develop a backlog of objects to be replicated, which can reduce the availability of read requests (write request availability is unaffected by replication).

In the catastrophic event that a cluster or site is unavailable, users and applications can still access content transparently via an HCP cluster at another location. In this configuration, HCP users are not affected even when a whole site or cluster is inaccessible.

> When you create a two-site cluster with replication, you can consider each cluster operating as redundant to the other. So the combined availability is calculated as $1-(1-99.9997\%)^2 = 99.9999999993\%$.

Two built-in capabilities provide transparent application failover using a second HCP cluster: (1) the application I/O is directed to the second cluster and (2) the data is accessible by the second cluster. HCP has multiple features for various configurations that support these capabilities:

Redirection to Second Cluster

If a whole site or cluster is inaccessible, then the **DNS failover** function automatically redirects application I/O from an inaccessible HCP cluster to a functioning HCP cluster, which may be at another site. Requests for content would then be serviced by the functioning cluster and conveyed back to the application or user. Alternatively, you can achieve similar effects using a load balancer. Or, configure the DNS infrastructure to choose among multiple HCP systems that use the same domain name based on geography and availability.

Let's say only some of the access nodes in the primary cluster are down, but all of them happen to be the nodes that oversee the requested data. In this case, the functioning access nodes may use the **read from remote** function, which tries to read the object from another cluster. The object is retrieved from the other cluster and the access node that was initially contacted responds to the request with the content.

Data Access at Second Cluster

The HCP administrator can choose between two methods for content to be stored at a second cluster: via a full replica of data ("**replication**") or by rebuilding content using fragments dispersed across clusters ("**geo-erasure coding**" or "geo-EC"). Replication provides fastest access but geo-EC requires up to 40% less storage than creating replicas.

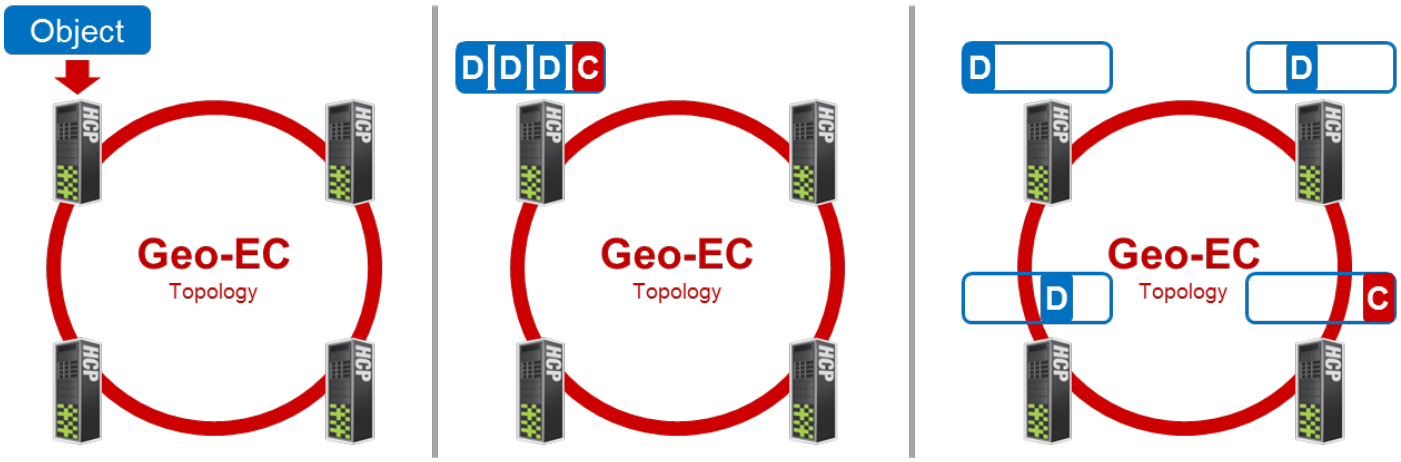
Replication (also known as "mirroring") is used to ensure that a full copy of data is stored at the other cluster; you can have replicas on multiple clusters. Accessing the replica content simply requires reading the data from the storage attached to the replica node. Replication between clusters can be configured as active/active or active/passive, and is performed asynchronously. This keeps the HCP I/O responsiveness high while still ensuring the content is protected quickly.

When you have at least three HCP clusters, a geo-erasure coding approach can save significant storage capacity compared to traditional replication (see Table 4). A portion of the data or a parity is stored at each cluster – not a full mirror. Content can be accessed by retrieving the available portions and parities from various clusters and then combining them to recreate the original data. Geo-EC includes a caching capability in which a node keeps a full copy of recently accessed objects locally to keep performance high when repeatedly accessing an object via geo-EC.

Table 4. Geo-EC Capacity Savings

Number of clusters	2	3	4	5	6
Geo-EC capacity savings vs a single mirror	0%	25%	33%	37%	40%

Figure 5. Chunk Movement Through an HCP Cluster in a Geo-EC Topology (Left-to-Right)



As shown in Figure 5, an object is ingested into a HCP cluster participating in a geo-erasure coding topology. Then, it is sliced into data chunks (D) and code chunks (C), and in the final state the chunks are distributed across all of the participating clusters (see Table 4).

HCP multisite clusters are designed to survive arbitrary network partitions while still guaranteeing a response for reads and writes. HCP uses an "eventual consistency" model between clusters, which provides high availability and informally guarantees that all accesses to an object will eventually return the last updated value. As changes propagate between clusters, HCP prioritizes the replication of metadata so that a node in active-active replication rapidly knows whether the local version of an object is out of date and where to retrieve the latest version. (Note

that using a strong consistency model across global clusters would have to sacrifice availability or performance to the point of impracticality.)

Beyond 15 Nines Durability: Replication and Geo-Erasure Coding

In addition to ensuring accessibility to content, replication and geo-EC between clusters also significantly improves the durability of data by adding off-site replicas. In the event that the original content is lost, the copies are available and can be used to rebuild the original. You can choose how many replicas you wish to make, and where you wish keep them based on performance, cost and resiliency requirements.

Much like the original content, the replicas also have high durability characteristics: They are stored on RAID systems or using erasure coding, and the content verification and scavenging services safeguard the data integrity. The replicas maintain the permissions and retention characteristics of the original, which prevents accidental, unauthorized or premature deletion.

Customer Example: Sabesp

Sabesp is among the largest water and waste management companies in the world, serving over 28 million people in São Paulo and 363 municipalities. About four years ago, Sabesp decided to modernize its storage infrastructure and integrate the file and content from 22 remote affiliates. They needed a reliable solution that accounted for various influences on water supply market, and set a contracted service level of 99.999% availability. The implementation of Hitachi Content Platform exceeded the service level agreement resulting in a full rollout into one of the largest file and content integration projects in Latin America. In the last four years, the Hitachi storage deployment has not experienced a single outage or data loss.

Conclusion: HCP = 10 Nines Accessibility + 15 Nines Durability

Hitachi Content Platform provides accessibility and durability appropriate for the core of an enterprise cloud. Applications and users should only expect ~3 milliseconds of downtime per year for a globally deployed system with 10 nines availability. Even deployments with massive numbers of objects have effectively zero chance of data loss thanks to the 15 nines' of data durability in an S node. Both planned downtime and unplanned downtime are virtually eliminated, providing a platform that IT can depend upon for critical applications and immense scale.

Hitachi Vantara

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HitachiVantara.com | community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com

WP-569-A T. Desai November 2017