(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 November 2015 (05.11.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/167320 A1

(51) International Patent Classification:
G06F 11/14 (2006.01) *G06F 11/20* (2006.01)
G06F 11/34 (2006.01)

(21) International Application Number:
PCT/MY2015/050022

(22) International Filing Date:
3 April 2015 (03.04.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI2014001220 28 April 2014 (28.04.2014) MY

(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(72) Inventors: **ISMAIL, Bukhary Ikhwan**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **KHALID, Mohammad Fairus**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **MOHD MYDIN, Mohd Nizam**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **ONG, Hong Hoe**; c/o Mimos Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(74) Agent: **MIRANDAH ASIA (MALAYSIA) SDN BHD**; Suite 3B-19-3, Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) **Title**: A SYSTEM AND METHOD FOR INTEGRATED BACKUP SOLUTION IN VIRTUALIZATION ENVIRONMENTS

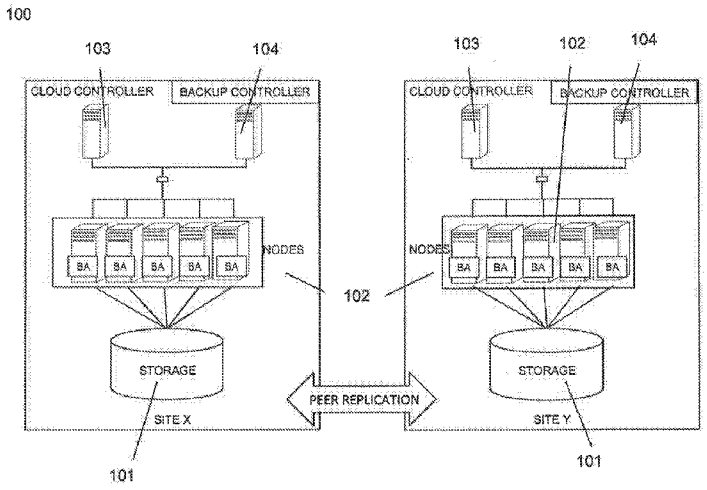


FIGURE 1

(57) **Abstract**: A system and method for integrated backup solution in virtualization environments makes use of the existing virtualization infrastructure to handle the backup process and peer with infrastructure at a different site for complying with business continuity requirements. The system (200) of the present invention comprising a Backup Controller (210) which further comprises a Web Service Interface (211) component that acts as an interface to the user; a Backup Engine (212) component that manages and coordinates the backup and restore process; a Host Monitor (214) component that monitors host load; a Replication Manager (213) component that manages the replication of backup images from a site to its peer site; a Backup Database (215) component that stores the backup information; a Backup Datastore (231) component that stores the backup information; and a Backup Agent (221) component that manages the backup activity at the node level. The objective of the present invention is achieved through visualization infrastructure to handle the backup process; and peering with infrastructure at a different site for complying with business continuity requirements.

WO 2015/167320 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

A SYSTEM AND METHOD FOR INTEGRATED BACKUP SOLUTION IN VIRTUALIZATION ENVIRONMENTS

FIELD OF INVENTION

The present invention relates to a system and method for integrated backup solution in virtualization environments. In particular, the invention relates to systems and methods that make use of the existing virtualization infrastructure to handle the backup process and peer with infrastructure at a different site for complying with business continuity requirements.

BACKGROUND ART

Introducing backup services in cloud computing environments requires a dedicated infrastructure (i.e. server(s) to execute back-up processes and storage to store the back-up elements). To comply with business continuity requirements, backed-up data needs to be replicated off-site for safety.

There are various problems associated with this process. For example, various issues may include the fact that the backup workload depends on how many and how frequent users are requesting such services. That is, requests are not consistent. There may be times where the number of backup activities requiring processing by the service provider is high while there are intervals where there is no backup workload to managed. A dedicated resource for backup operation may need to be planned up front. Under commissioning will generally result in long queues of backup operation waiting to be serviced. This will impact the Service Level Agreement (SLA) in place with the end users. Over commissioning will result in wastage through idle resources.

United States Patent No. 8,387,054 B1 discloses a method and apparatus for scheduling data movers is described. The method and apparatus comprise monitoring utilization of a resource used by a data mover to process a data flow, determining rank information based on the utilization of the resource and scheduling a task according to the rank

information. This document discloses a method in which backup and restore operations are executed on the highest ranked BA.

United States Patent No. 8,046,550 B2 describes backup systems and methods for a virtual computing environment. Certain examples include a system having a backup management server that communicates with a host server having at least one virtual machine. The management server coordinates with the host server to perform backup copies of entire virtual machine disks from outside the guest operating system of the virtual machine. In certain examples, such backup systems further utilize a volume shadow copy service executing on the host server to quiesce virtual machine applications to put data in a consistent state to be backed up. The backup system then utilizes hypervisor snapshot capabilities of the host server to record intended changes to the virtual machine disk files while such files are being copied (e.g., backed up) by the host server. Such recorded changes can be later committed to the virtual machine disk files once the backup operation has completed. This document discloses systems and methods in which backup and restore operations are executed on a single external machine.

The publication iROW: An Efficient Live Snapshot System for Virtual Machine Disk (ICPADS), 2012 IEEE 18th International Conference on Parallel and Distributed Systems, Pages 376-383, suggests that the high-availability of mission-critical data and services hosted in a virtual machine (VM) is one of the top concerns in a cloud computing environment. In the iROW publication, for each of backup and restore operation, consistent state is requested. Virtual Machine is snapshot and the backup operation is executed on a single external machine which improves the copy-and-write snapshot mechanism.

The overall objective of the present invention is achieved through virtualization infrastructure to handle the backup process; and peering with infrastructure at a different site for complying with business continuity requirements.

SUMMARY OF INVENTION

The present invention relates to a system and method for integrated backup solution in virtualization environments. In particular, the present invention relates to systems and methods which distributes backup process workload across nodes and replicates the backup image into peer sites.

One aspect of the present invention provides a system for distributed backup of workload across nodes and replication of backup information into peer sites, the system comprising a Backup Controller comprising a Web Service Interface component that acts as an interface to the user; a Backup Engine component that manages and coordinates the backup and restore process; a Host Monitor component that monitors host load; a Replication Manager component that manages the replication of backup images from a site to its peer site; a Backup Database component that stores the backup information; a Backup Datastore component that stores the backup information; and a Backup Agent component that manages the backup activity at the node level.

Another aspect of the present invention provides a system wherein the backup information comprises backup images, corresponding virtual machine (VM) images and backup image chunks.

A further aspect of the present invention provides a method for distributed backup of workload across nodes and replication of backup information into peer sites, the method comprising receiving a request to backup a VM from a user; locating the VM to backup; flushing the VM system state into a VM image; taking a snapshot of the VM image and copying it into a Backup Datastore as a backup image; assigning a least loaded node to split the backup image into a plurality of backup image chunks; informing Backup Agents in all nodes to start the backup process; and storing backup information into a Backup Database.

Yet another aspect of the present invention provides a method wherein the backup information comprises the backup image chunks.

Still another aspect of the present invention provides a method wherein informing Backup Agents in all nodes to start the backup process further comprises steps of receiving a request to process backup from a Backup Controller; checking the node has resource capacity to process a backup image chunk; checking there is a backup image chunk available to be processed; if available, processing a backup image chuck; and informing the Backup Controller of the outcome of the process.

Another aspect of the present invention provides a method wherein the processing of the backup image chunk comprises but not limited to compression, encryption or deduplication of the backup image chunks.

A further aspect of the present invention provides a method wherein a Replication manager manages the replication of backup images to peer sites, the replication management comprising detecting the availability of processed backup images; identifying a configurable number of nodes with least load; informing a peer site to prepare a similar number of nodes to accept file transfer; parallel transferring the backup images to the peer site; and updating the backup information in the Backup Database.

Another aspect of the present invention is provided with a restoring process which manages the restoration of backed up images, the restore process comprising receiving a restore VM request from user; locating the backup image; informing the Backup Agent in all the nodes to start reversing the backup process; assigning the least loaded node to merge the backup image chunks; copying the backup image into an Image Datastore; informing a Cloud Controller to launch the copied backup image; and updating the backup information in the Backup Database.

Yet another aspect of the present invention provides a method wherein the reversing of the backup process comprises decryption or uncompressing of the backup image chunks.

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various

changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

FIG. 1 illustrates a distributed backup context of a system according to an embodiment of the invention.

FIG. 2 illustrates distributed backup component architecture of a system according to an embodiment of the invention.

FIG. 3 illustrates the backup process of a system according to an embodiment of the invention.

FIG. 4 illustrates the architecture of the backup process of the present invention.

FIG. 4a illustrates a backup process simulation of a system according to an embodiment of the invention.

FIG. 5 illustrates a backup agent process of a system according to an embodiment of the invention.

FIG. 6 illustrates a backup replication process of a system according to an embodiment of the invention.

FIG. 7 illustrates a backup replication simulation of a system according to an embodiment of the invention.

FIG. 8 illustrates a restore process of a system according to an embodiment of the invention.

FIG. 9 illustrates a restore process simulation of a system according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention relates to a system and method for integrated backup solution in virtualization environments. In particular, the invention relates to systems and methods that make use of the existing virtualization infrastructure to handle the backup process and peer with infrastructure at a different site for complying with business continuity requirements. To integrate the backup service into the virtualization infrastructure and minimize the impact of backup/restore workload, the backup data is segmented into smaller predefined sizes and the workload is distributed amongst the nodes. Nodes with insufficient processing capacity are not be used as processing nodes.

Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

Referring to Figure 1, a simple distributed backup context design 100 is illustrated. This includes a pair of sites, X and Y, storage 101, a plurality of nodes 102, a cloud controller 103 and backup controller 104. Further discussion of these components will be described in the following description of the subsequent Figures.

Referring to Figure 2, a system 200 of an embodiment of the invention is illustrated in more detail below. The system 200 comprises a backup controller 210 that includes a web service interface 211, a backup engine 212, a replication manager 213, a host monitor 214 and a backup database 215. The system 200 also includes at least one backup agent 221 associated with at least one node 220. Each node comprises a hypervisor 222 and is designated, as illustrated, with associated virtual machines VM_1, VM_2,.....VM_n. Storage 230 is also provided and includes a backup datastore 231 and a VM image datastore 232.

The backup methodology according to an embodiment of the invention is illustrated by way of flowchart in Figure 3. According to the backup method 300, a backup controller (BC) receives a request 301 from a user to backup a virtual machine (VM). Prior to the

initiation of the backup, the user must ensure proper handling of application data or application transactions to be properly flush or stored in the disk at the time snapshot is taken. The backup engine (BE) locates the VM to backup 302 and sends a command to the hypervisor to flush the system states into the VM image 303. The BE then sends a command to the hypervisor to take a snapshot of the VM 304 and copies the snapshot delta into the backup datastore 305. The duration of the copying process is subjected to the size of the snapshot delta.

The host monitor then identifies the node with least load 306 and the BE sends a command to the backup agent (BA) of the identified node to split the backup delta 307. The delta is split into predefined chunks 308 and the BA informs the BE on completion of this process 309. The BE then broadcasts to all BA with "sufficient resources" to start processing the chunks of backup delta 310. "Sufficient resources" is a server with enough CPU, memory, storage I/O, etc resources. The data process may involve which is not limited to deduplication, compression and encryption, as previously described. Finally, the BE stores the backup information in the backup database 311.

The methodology of Figure 3 is illustrated further in Figure 4 and Figure 4a. Figure 4 illustrates the architecture of the backup process while Figure 4a illustrates a backup process simulation according to this embodiment of the invention. In this illustration, a backup request is received 401. The backup engine 412 locates the requested VM 402 on node 420'. The BE 412 requests that the hypervisor 422' flush the system state 403. The BE 412 then sends a command to the hypervisor 422' to snapshot the VM 404 and copies the snapshot delta 405 into the backup store 431.

The host monitor 414 finds 406 the least load node 420''. The BE 412 sends a command to the backup agent 421'' of the node 420'' to split the delta 407.The BA 421'' informs the BE 412 on completed status 409. The BE 412 broadcasts to all BA 421" with sufficient resources to process the chunks of backup delta 410.

Referring to Figure 5, a backup agent process 500 is illustrated. The backup agent process 500 comprises initial receipt by the BA of a request to start the backup process from the BE 501, followed by checking the node has resource capacity to process a

backup image chunk 502. If not, the BA informs the BE 503. If the node does have capacity, a check is conducted to determine if there is a backup image chunk available to be processed 504. If available, the backup image chuck is marked for processing 505 and processed 506. Once the process is completed, the chunk is marked as processed. 507.

The methodology for distributed backup of workload across nodes and replication of backup information into peer sites further comprising managing replication of backup images to peer sites. The backup replication methodology 600 is illustrated in Figure 6. Referring to this figure, the replication manager (RM) detects the availability of processed backup images 601. It then identifies a configurable number of nodes with "least load" 602 and informs the peer backup controller (BC) 603. . "Least load" nodes is a server in which its CPU, memory, storage I/O, etc is not under heavy load. The peer BC prepares a similar number of nodes with least load to accept replication and inform the RM 604. The RM then informs the BA of the identified nodes to start parallel transferring of the backup images to the peer site 605. Subsequently, the RM updates the backup information in the backup database 606 and the peer BC updates the backup information in the Backup Database 607.

The methodology of Figure 6 is illustrated further in Figure 7, which illustrates a backup replication simulation 700 according to this embodiment of the invention. As previously described, the process involves initial detection of availability of processed backup data 701 by the RM 713. The RM 713 then identifies local nodes with least load 702 and informs BC 710 for the replication process 703. The peer RM 713' finds a similar number of nodes with least load to accept replication 704 and informs the BA to start the parallel transfer of data 705. The source RM 713 updates the backup information 706 in the backup database 715 and the peer RM 713' updates the backup information in the peer backup database 715'.

Referring to Figure 8, a restoring process 800 is illustrated. The restoring process is a further step from the methodology for distributed backup of workload across nodes and replication of backup information into peer sites further comprising managing replication of backup images to peer sites. The process 800 generally includes receiving a restore

VM request from a user 801. The BE then finds the backup information from the backup database 802 and identifies whether the information is found 803. If not, the BE queries the peer BC 804 and determines whether information is found 805. If not, the peer BC replies to the query accordingly 806. If so, the peer BC initiates the transfer process 807 and replies to the query and updates both backup databases 808.

If the information is found, the BE informs all Backup Agents in all the nodes to start reversing the backup process by uncompressing and decrypting the chunks backup data 809. The host monitor then assigns the least loaded node 810 to merge the backup image chunks 811. The BA merges the backup image into an Image Datastore 812, and the BE copies the backup image from the backup datastore to the image datastore 813. The BE then informs the Cloud Controller to launch the copied backup image 814.

The methodology of Figure 8 is illustrated further in Figure 9, which illustrates a backup replication simulation 900 according to this embodiment of the invention. As illustrated in Figure 9, BA receives request to restore data 902. Thereafter, BE locates backup information from Backup Database 904 and broadcast to all BAs to process the chunks by decrypting and uncompressing the information. The Host Monitor finds out the host with the least node 908 and further sends command to the BA of the identified node to merge the chunks of the backup image 910. Subsequently, BE copies the backup image to Image Datastore 912.

The present invention manages backup workload by enabling a Cloud Computing operator to optimize the usage of existing infrastructure. The present invention further provides backup services to cloud users by making use of the existing virtualization infrastructure to handle the backup process; and peering with infrastructure at a different site for complying with business continuity requirements.

Unless the context requires otherwise or specifically stated to the contrary, integers, steps or elements of the invention recited herein as singular integers, steps or elements clearly encompass both singular and plural forms of the recited integers, steps or elements.

Throughout this specification, unless the context requires otherwise, the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated step or element or integer or group of steps or elements or integers, but not the exclusion of any other step or element or integer or group of steps, elements or integers. Thus, in the context of this specification, the term "comprising" is used in an inclusive sense and thus should be understood as meaning "including principally, but not necessarily solely".

It will be appreciated that the foregoing description has been given by way of illustrative example of the invention and that all such modifications and variations thereto as would be apparent to persons of skill in the art are deemed to fall within the broad scope and ambit of the invention as herein set forth.

CLAIMS

1. A system (200) for distributed backup of workload across nodes and replication of backup information into peer sites, the system comprising:

a Backup Controller (210) comprising:

a Web Service Interface (211) component that acts as an interface to the user;

a Backup Engine (212) component that manages and coordinates the backup and restore process;

a Host Monitor (214) component that monitors host load;

a Replication Manager (213) component that manages the replication of backup images from a site to its peer site;

a Backup Database (215) component that stores the backup information;

a Backup Datastore (231) component that stores the backup information; and

a Backup Agent (221) component that manages the backup activity at the node level.

2. A system (200) as claimed in claim 1, wherein said backup information comprises backup images, corresponding virtual machine (VM) images and backup image chunks.

3. A method (300) for distributed backup of workload across nodes and replication of backup information into peer sites, the method comprising:

receiving a request to backup a VM from a user (301);

locating the VM to backup (302);

flushing the VM system state into a VM image (303);

taking a snapshot of the VM image (304) and copying it into a Backup Datastore as a backup image (305);

assigning a least load node to split the backup image into a plurality of backup image chunks (306);

informing Backup Agents in all nodes to start the backup process (307); and

storing backup information into a Backup Database (311)

4. A method (300) as claimed in claim 3, wherein said backup information comprises said backup image chunks.

5. A method (300) as claimed in claim 3, wherein informing Backup Agents in all nodes to start the backup process further comprising steps of:

receiving a request to process backup from a Backup Engine (501);

checking the node has resource capacity to process a backup image chunk (502);

checking there is a backup image chunk available to be processed (504);

if available, processing a backup image chuck (505); and

informing the Backup Controller of the outcome of the process (503).

6. A method (300) as claimed in claim 5, wherein said processing of said backup image chunk comprises compression, encryption or deduplication of said backup image chunks.

7. A method (300) as claimed in claim 3, further comprising managing replication of backup images to peer sites, the replication process further comprising steps of:

detecting the availability of processed backup images (601);

identifying a configurable number of nodes with least load (602);

informing a peer site to prepare a similar number of nodes to accept file transfer (603);

parallel transferring the backup images to the peer site (604); and

updating the backup information in the Backup Database (606, 607).

8. A method as claimed in claim 3, is provided with a restoring process which manages the restoration of backed up images, the restoring process comprising steps of:

receiving a restore VM request from user (801);

locating the backup image (802);
informing the Backup Agent in all the nodes to start reversing the backup process (809);
assigning the least load node to merge the backup image chunks (811);
copying the backup image into an Image Datastore (813);
informing a Cloud Controller to launch the copied backup image (814); and
updating the backup information in the Backup Database.

9. A method as claimed in claim 8, wherein said reversing of the backup process (809) comprises decryption or uncompressing of said backup image chunks.

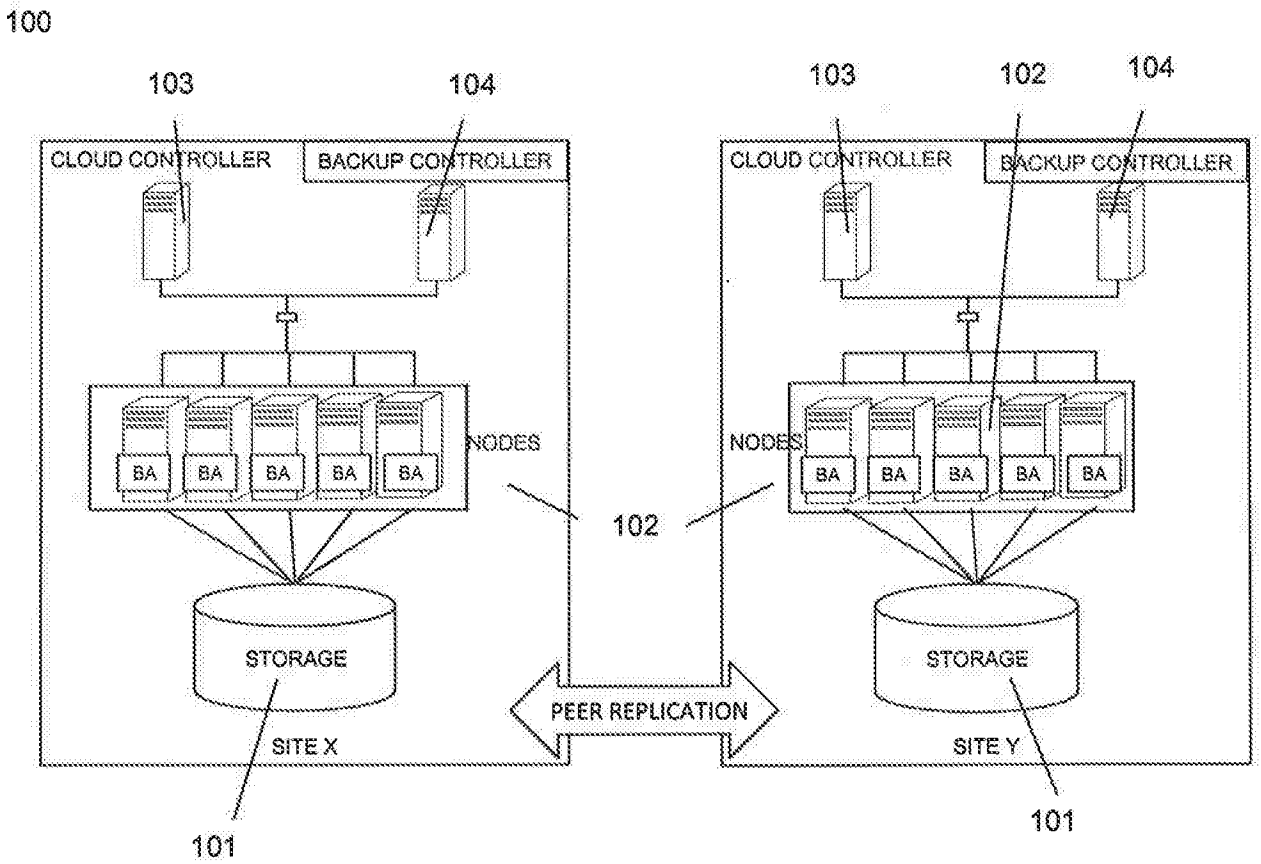

100
103
104
103
102
104
CLOUD CONTROLLER
BACKUP CONTROLLER
CLOUD CONTROLLER
BACKUP CONTROLLER
NODES
NODES
BA
BA
BA
BA
BA
BA
BA
BA
BA
BA
102
STORAGE
STORAGE
PEER REPLICATION
SITE X
SITE Y
101
101

FIGURE 1

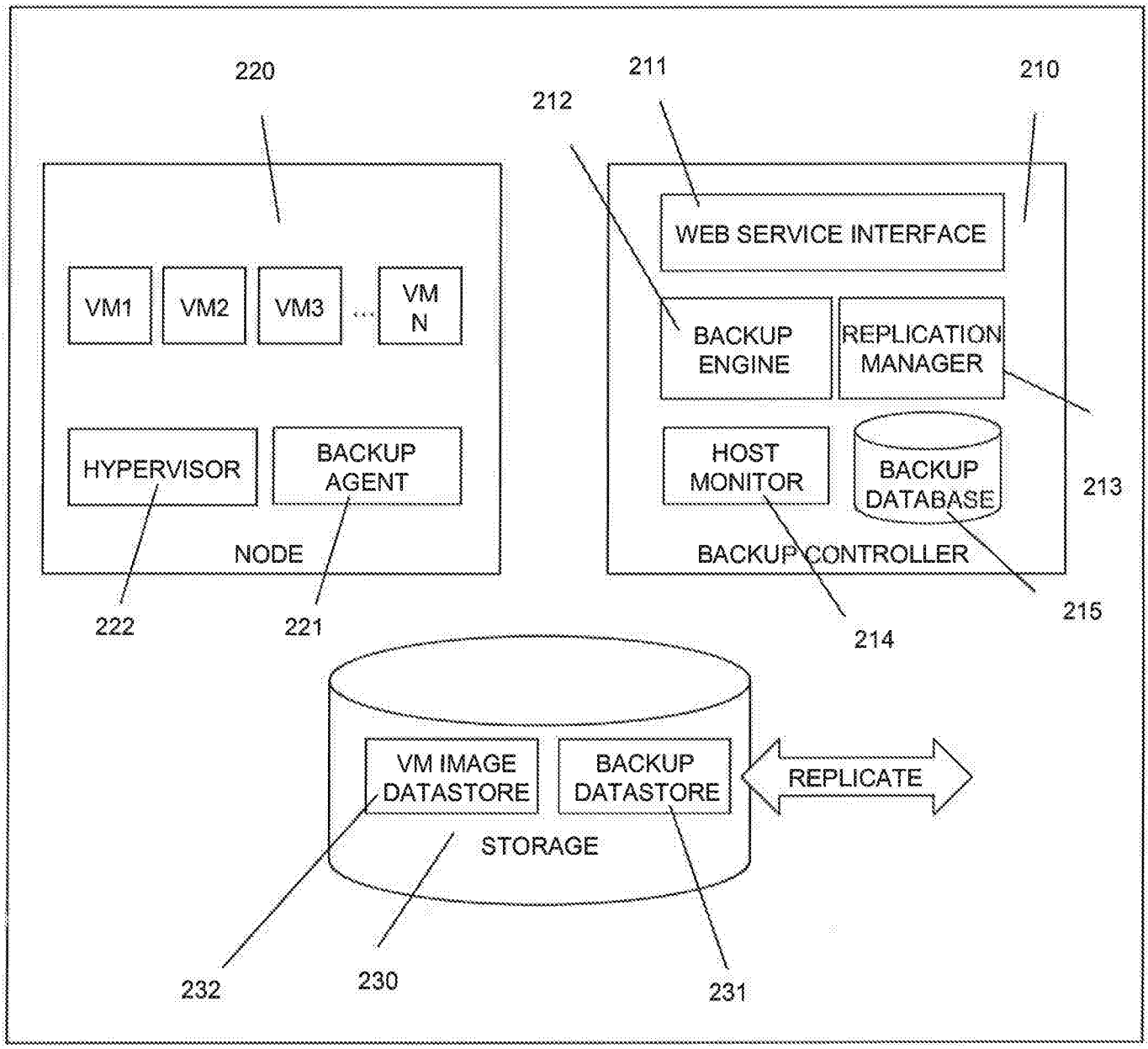

200
220
211
212
210
VM1
VM2
VM3
...
VM N
WEB SERVICE INTERFACE
BACKUP ENGINE
REPLICATION MANAGER
HYPERVISOR
BACKUP AGENT
HOST MONITOR
BACKUP DATABASE
213
NODE
BACKUP CONTROLLER
222
221
214
215
VM IMAGE DATASTORE
BACKUP DATASTORE
REPLICATE
STORAGE
232
230
231

FIGURE 2

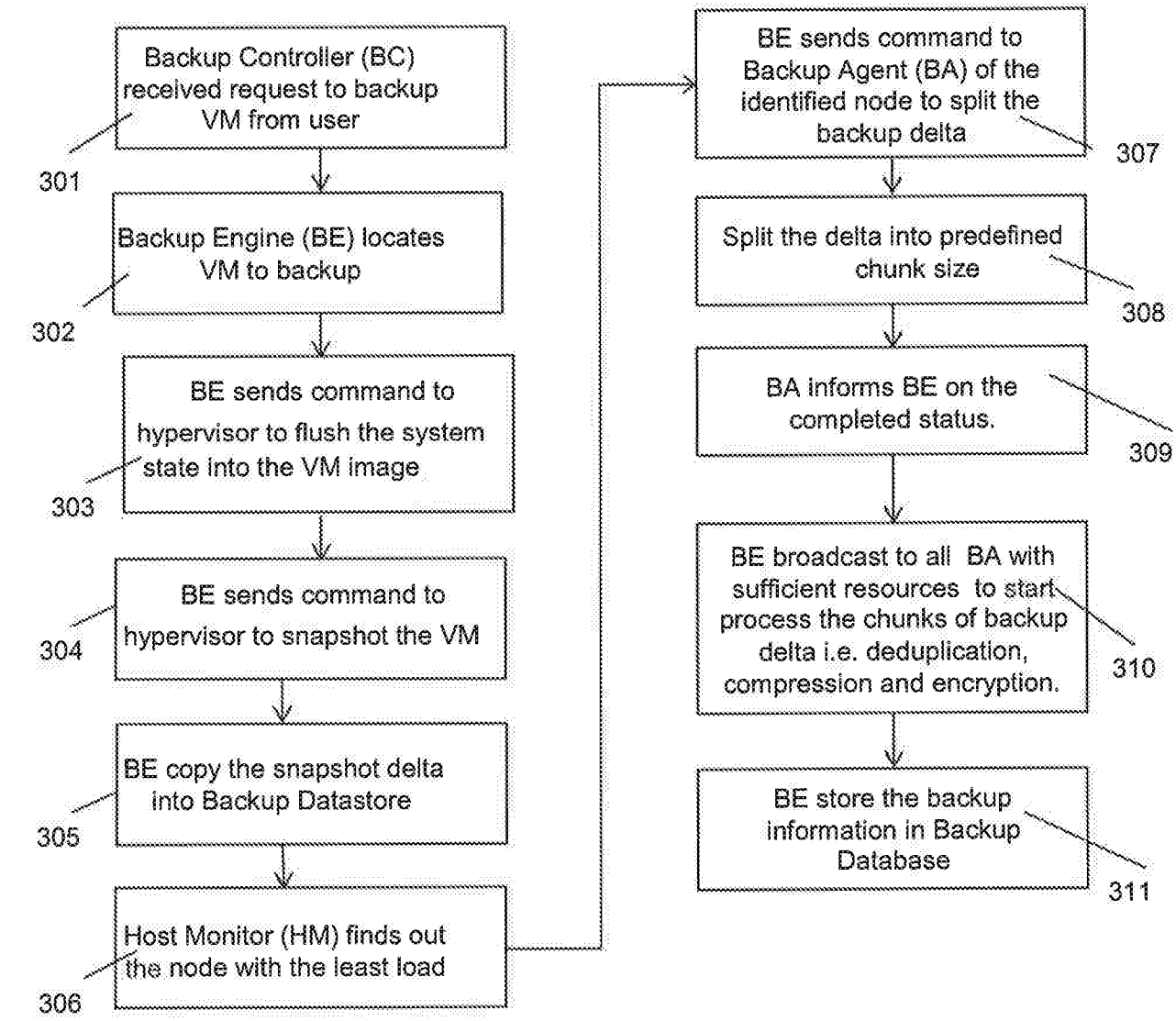

300
Backup Controller (BC) received request to backup VM from user
301
Backup Engine (BE) locates VM to backup
302
BE sends command to hypervisor to flush the system state into the VM image
303
BE sends command to hypervisor to snapshot the VM
304
BE copy the snapshot delta into Backup Datastore
305
Host Monitor (HM) finds out the node with the least load
306
BE sends command to Backup Agent (BA) of the identified node to split the backup delta
307
Split the delta into predefined chunk size
308
BA informs BE on the completed status.
309
BE broadcast to all BA with sufficient resources to start process the chunks of backup delta i.e. deduplication, compression and encryption.
310
BE store the backup information in Backup Database
311

FIGURE 3

400

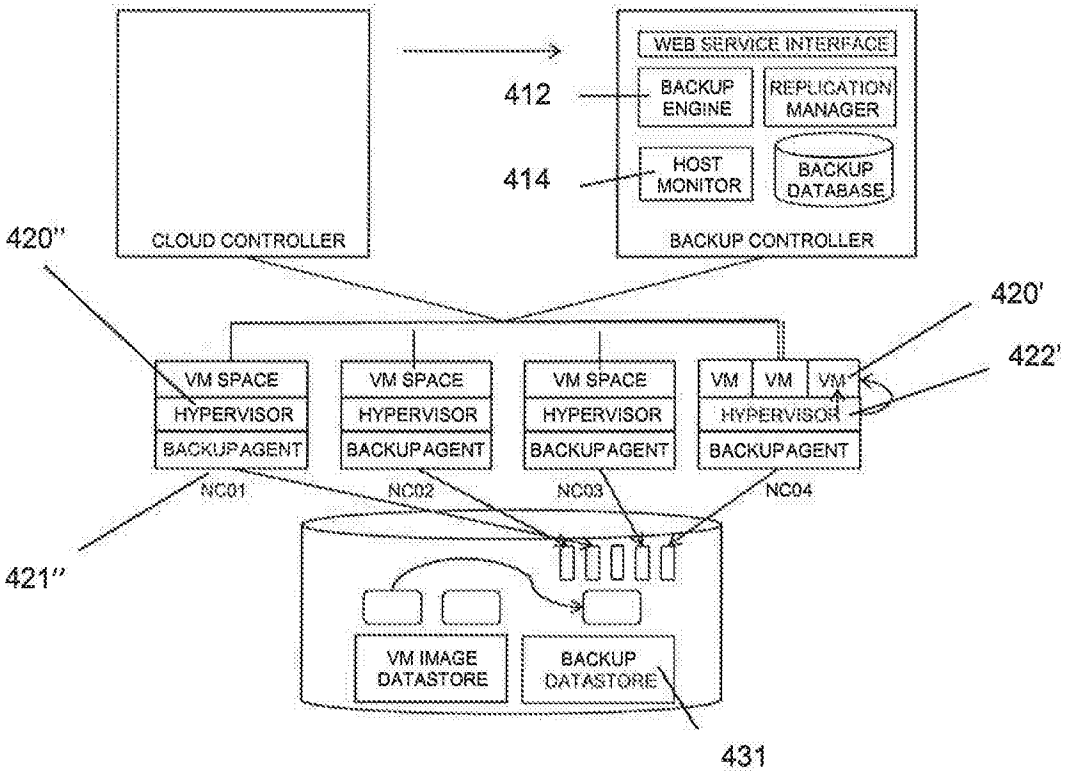

WEB SERVICE INTERFACE
412
BACKUP ENGINE
REPLICATION MANAGER
414
HOST MONITOR
BACKUP DATABASE
CLOUD CONTROLLER
BACKUP CONTROLLER
420''
420'
422'
VM SPACE
HYPERVISOR
BACKUP AGENT
VM
NC01
NC02
NC03
NC04
421''
VM IMAGE DATASTORE
BACKUP DATASTORE
431

FIGURE 4

400a

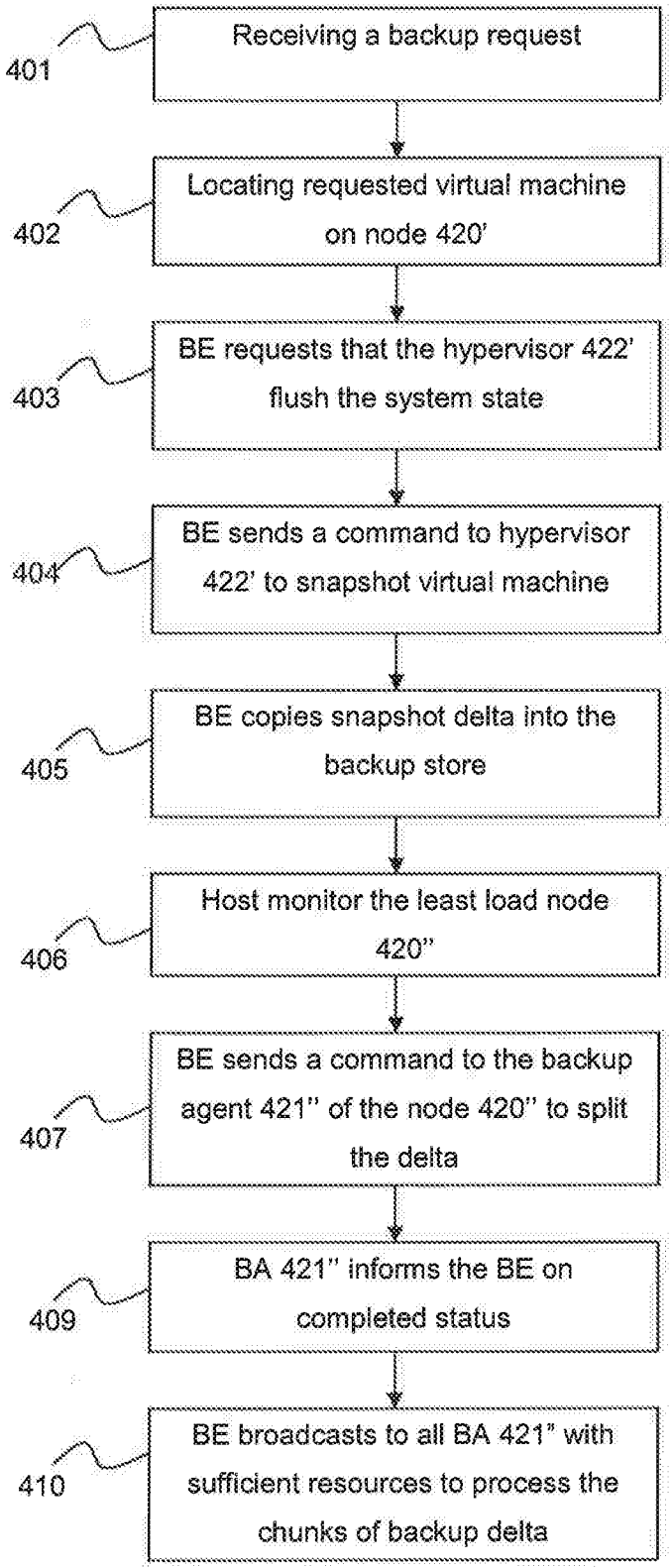


FIGURE 4A

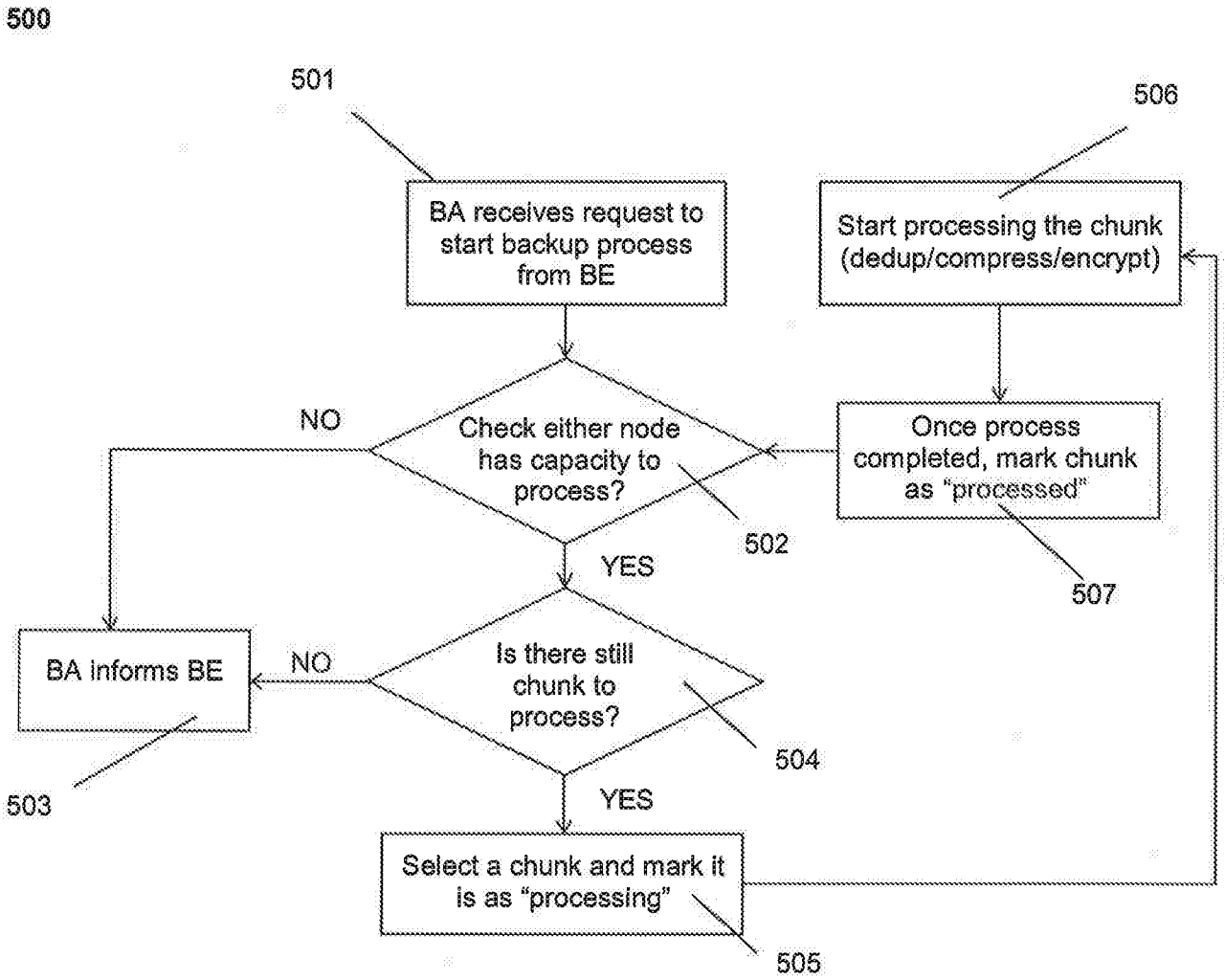

500
501
BA receives request to start backup process from BE
506
Start processing the chunk (dedup/compress/encrypt)
Check either node has capacity to process?
NO
YES
502
Once process completed, mark chunk as "processed"
507
BA informs BE
NO
Is there still chunk to process?
504
503
YES
Select a chunk and mark it is as "processing"
505

FIGURE 5

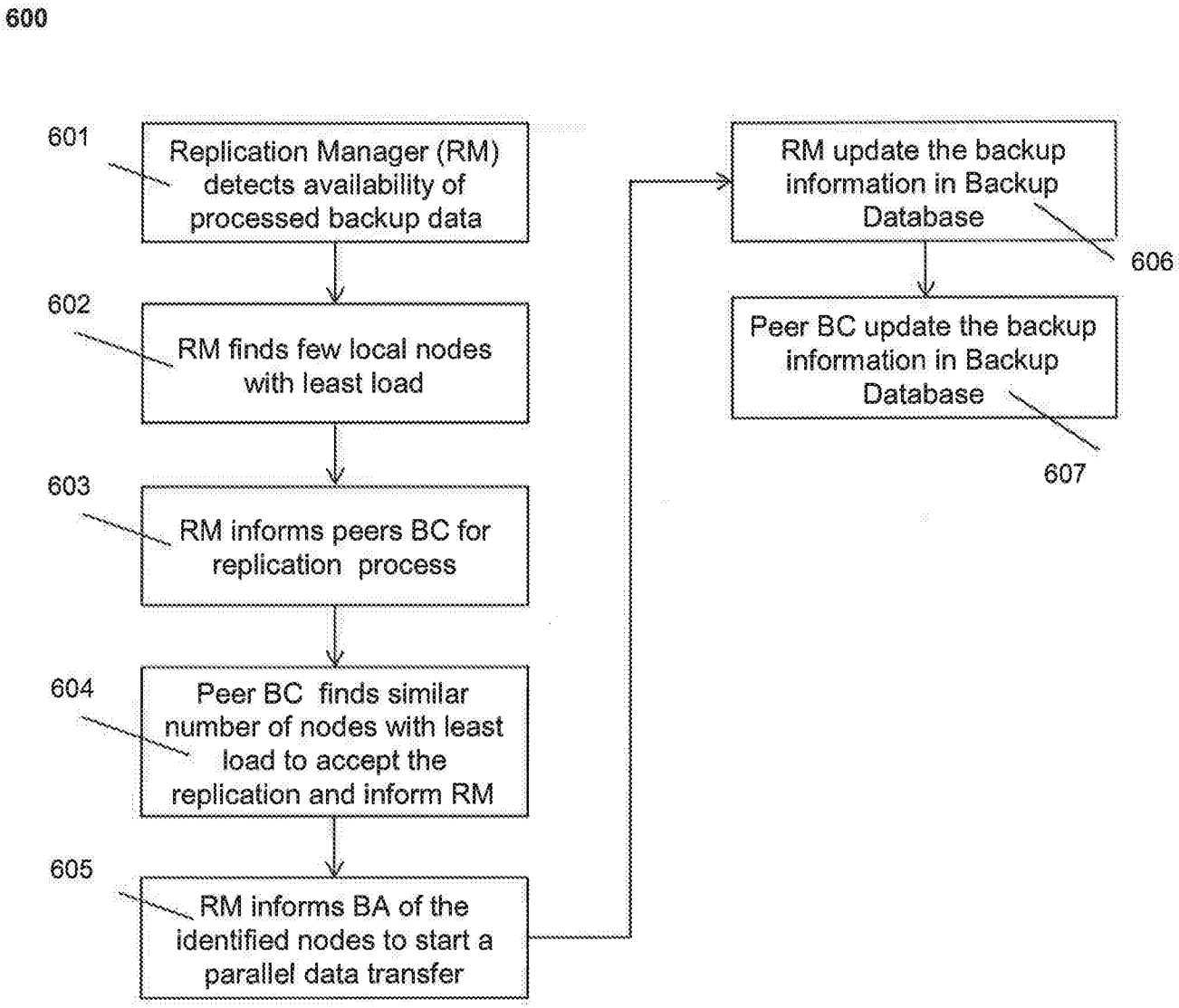

600
601
Replication Manager (RM) detects availability of processed backup data
602
RM finds few local nodes with least load
603
RM informs peers BC for replication process
604
Peer BC finds similar number of nodes with least load to accept the replication and inform RM
605
RM informs BA of the identified nodes to start a parallel data transfer
RM update the backup information in Backup Database
606
Peer BC update the backup information in Backup Database
607

FIGURE 6

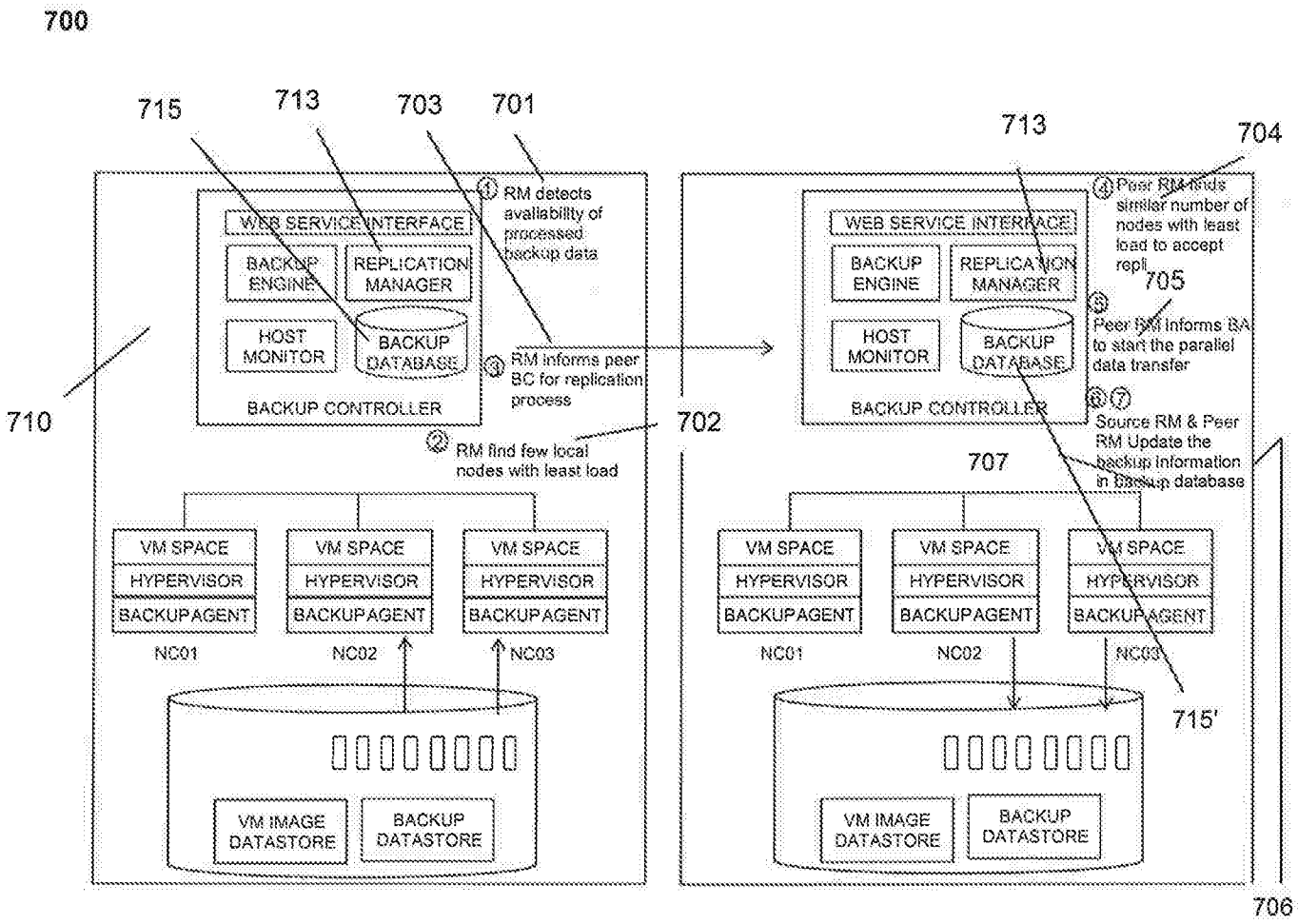

700
715
713
703
701
713
704
710
702
707
705
706
715'
WEB SERVICE INTERFACE
BACKUP ENGINE
REPLICATION MANAGER
HOST MONITOR
BACKUP DATABASE
BACKUP CONTROLLER
1 RM detects availability of processed backup data
3 RM informs peer BC for replication process
2 RM find few local nodes with least load
4 Peer RM finds similar number of nodes with least load to accept repli
5 Peer BM informs BA to start the parallel data transfer
6 7 Source RM & Peer RM Update the backup information in backup database
VM SPACE
HYPERVISOR
BACKUPAGENT
NC01
NC02
NC03
VM IMAGE DATASTORE
BACKUP DATASTORE

FIGURE 7

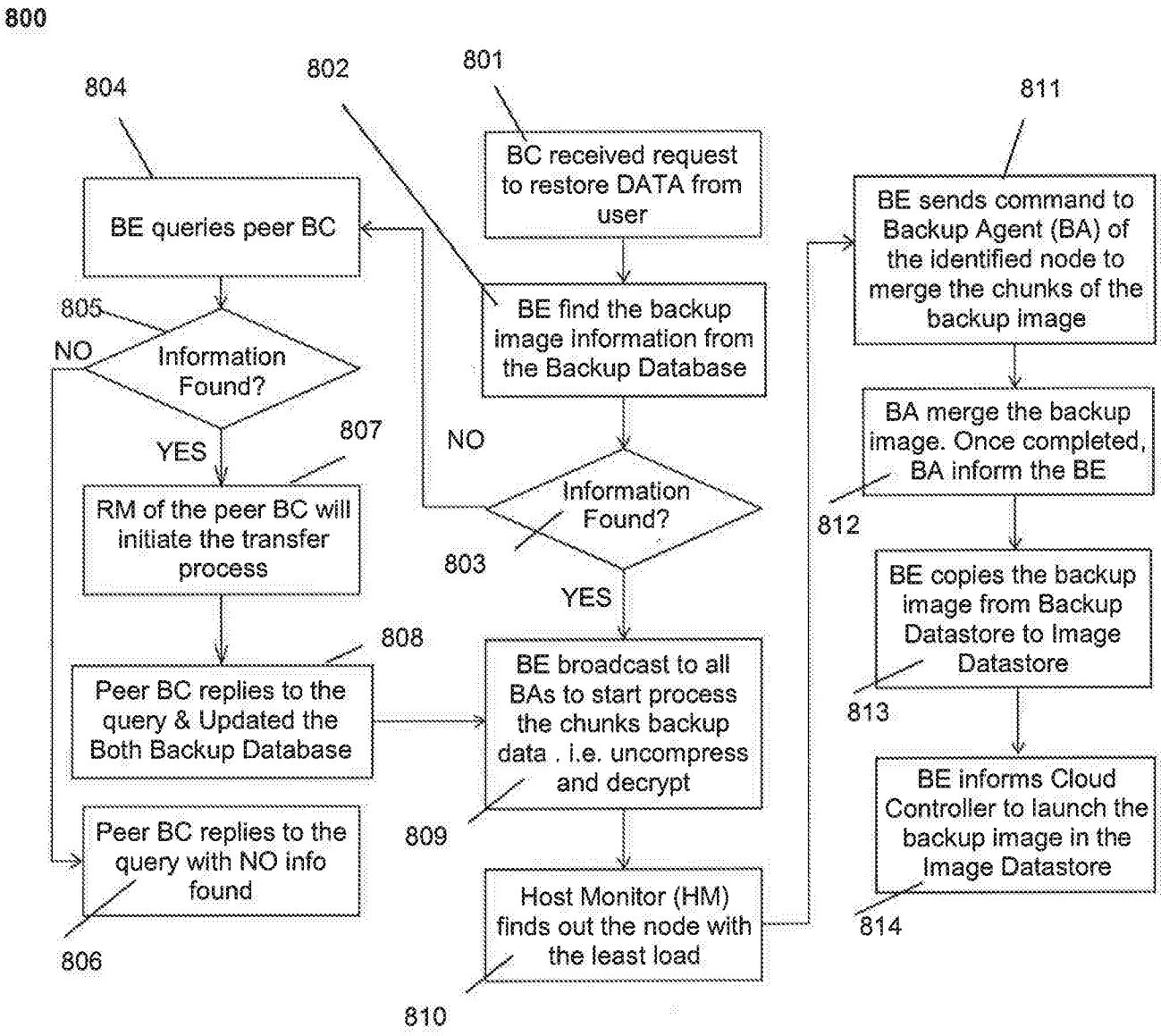

800
804
802
801
811
BE queries peer BC
BC received request to restore DATA from user
BE sends command to Backup Agent (BA) of the identified node to merge the chunks of the backup image
805
NO
Information Found?
BE find the backup image information from the Backup Database
BA merge the backup image. Once completed, BA inform the BE
807
YES
NO
812
RM of the peer BC will initiate the transfer process
Information Found?
803
BE copies the backup image from Backup Datastore to Image Datastore
YES
808
Peer BC replies to the query & Updated the Both Backup Database
BE broadcast to all BAs to start process the chunks backup data . i.e. uncompress and decrypt
813
BE informs Cloud Controller to launch the backup image in the Image Datastore
Peer BC replies to the query with NO info found
809
Host Monitor (HM) finds out the node with the least load
814
806
810

FIGURE 8

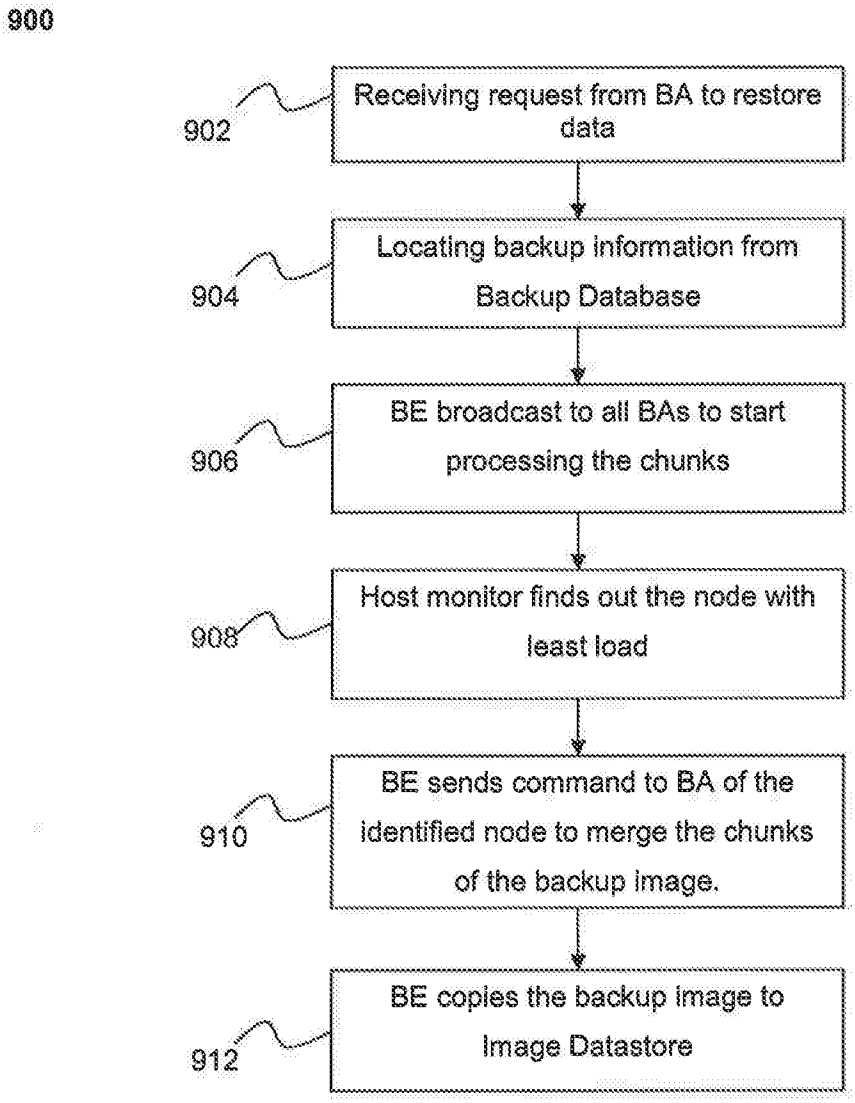

900
902
Receiving request from BA to restore data
904
Locating backup information from Backup Database
906
BE broadcast to all BAs to start processing the chunks
908
Host monitor finds out the node with least load
910
BE sends command to BA of the identified node to merge the chunks of the backup image.
912
BE copies the backup image to Image Datastore

FIGURE 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2015/050022

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F11/14 G06F11/34
ADD. G06F11/20

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 7 552 358 B1 (ASGAR-DEEN TERRENCE [US] ET AL) 23 June 2009 (2009-06-23) page 1, lines 31-38 page 3, line 64 - page 5, line 39 page 9, line 54 - page 11, line 54 figures 1,3 -----	1,2
Y	US 2011/029748 A1 (NAKAMURA SADAHIRO [JP] ET AL) 3 February 2011 (2011-02-03) abstract figures 1,2,28 paragraph [0068] - paragraph [0071] paragraph [0083] - paragraph [0085] paragraph [0116] - paragraph [0119] paragraph [0195] - paragraph [0197] ----- -/--	1,2

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 July 2015	30/09/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Lanchès, Philippe

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2015/050022

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2012/284236 A1 (TIMASHEV RATMIR [CH] ET AL) 8 November 2012 (2012-11-08) paragraph [0004] - paragraph [0006]	2
A	US 2003/217068 A1 (FRUCHTMAN BARRY [US] ET AL) 20 November 2003 (2003-11-20) paragraph [0004] - paragraph [0006]	1,2
A	EP 1 217 543 A1 (HEWLETT PACKARD CO [US]) 26 June 2002 (2002-06-26) paragraph [0033] - paragraph [0037]	1,2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2015/050022

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1, 2

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1, 2

   Backup replication architecture for a distributed system.

   ---

2. claims: 3-9

   Consistent virtual machine backup using multiple nodes.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/MY2015/050022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7552358 B1	23-06-2009	US 7552358 B1	23-06-2009
		US 7657582 B1	02-02-2010
		US 7672979 B1	02-03-2010
		US 7761456 B1	20-07-2010
		US 7822726 B1	26-10-2010
		US 8032491 B1	04-10-2011
US 2011029748 A1	03-02-2011	JP 2011034164 A	17-02-2011
		US 2011029748 A1	03-02-2011
US 2012284236 A1	08-11-2012	EP 2596426 A2	29-05-2013
		US 2012017114 A1	19-01-2012
		US 2012284236 A1	08-11-2012
		US 2014047268 A1	13-02-2014
		WO 2012012365 A2	26-01-2012
US 2003217068 A1	20-11-2003	NONE	
EP 1217543 A1	26-06-2002	EP 1217543 A1	26-06-2002
		US 2002083053 A1	27-06-2002