Notice

DESCRIPTION CN112527567A

System disaster recovery method, device, equipment and storage medium

[0001]

Technical Field

[n0001]

The present application relates to the field of computer technology, specifically to the field of cloud computing and small program technology, and especially to a system disaster recovery method, device, equipment and storage medium.

[0003]

Background Art

[n0002]

In actual applications, any system may become unavailable if a power outage, network interruption, or software error (bug) occurs during use.
For distributed storage systems, a storage replication relationship is often established between two clusters, that is, the data on the primary cluster is copied to the backup cluster through a replication link to cope with the problem that the system cannot provide services when a single cluster fails, thereby ensuring the high availability of the system.

[0005]

Summary of the invention

[n0003]

Provided are a system disaster recovery method, apparatus, device and storage medium.

[n0004]

According to a first aspect, a system disaster recovery method is provided, comprising: in response to determining that a primary cluster in the system has failed, determining whether a backup cluster in the system is available; in response to determining that the backup cluster is available, modifying cluster configuration information; and outputting the modified cluster configuration information to a user of the primary cluster, so that the user uses the backup cluster according to the modified cluster configuration information.

[n0005]

According to a second aspect, a system disaster recovery device is provided, comprising: a state determination unit, configured to determine whether a backup cluster in the system is available in response to determining that a primary cluster in the system has failed; an information modification unit, configured to modify cluster configuration information in response to determining that the backup cluster is available; and an information output unit, configured to output the modified cluster configuration information to a user of the primary cluster, so that the user can use the backup cluster according to the modified cluster configuration information.

[n0006]

According to a third aspect, a system disaster recovery electronic device is provided, comprising: at least one computing unit; and a storage unit communicatively connected to the at least one computing unit; wherein the storage unit stores instructions executable by the at least one computing unit, and the at least one computing unit executes the instructions so that the at least one computing unit can execute the method described in the first aspect.

[n0007]

According to a fourth aspect, a non-transitory computer-readable storage medium storing computer instructions is provided, wherein the computer instructions are used to cause a computer to execute the method described in the first aspect.

[n0008]

According to a fifth aspect, a computer program product comprises a computer program, and when the computer program is executed by a computing unit, the computer program implements the method described in the first aspect.

[n0009]

According to the technology of the present application, a system disaster recovery method is provided, which can modify the system configuration information when the main cluster fails, and output it to the user who calls the main cluster, so that the user can modify the configuration according to the system configuration information, thereby switching to an available backup cluster, thereby improving the high availability of the system.

[n0010]

It should be understood that the content described in this section is not intended to identify key or important features of the embodiments of the present disclosure, nor is it intended to limit the scope of the present disclosure.
Other features of the present disclosure will become readily understood from the following description.

[0014]

BRIEF DESCRIPTION OF THE DRAWINGS

[n0011]

The accompanying drawings are used to better understand the present solution and do not constitute a limitation of the present application.
in:

[n0012]

FIG1 is an exemplary system architecture diagram in which an embodiment of the present application can be applied;

[n0013]

FIG2 is a flow chart of an embodiment of a system disaster recovery method according to the present application;

[n0014]

FIG3 is a schematic diagram of an application scenario of the system disaster recovery method according to the present application;

[n0015]

FIG4 is a flow chart of another embodiment of a system disaster recovery method according to the present application;

[n0016]

FIG5 is a schematic structural diagram of an embodiment of a system disaster recovery device according to the present application;

[n0017]

FIG6 is a block diagram of an electronic device for implementing the system disaster recovery method according to an embodiment of the present application.

[0022]

DETAILED DESCRIPTION

[n0018]

The following describes exemplary embodiments of the present application in conjunction with the accompanying drawings, which include various details of the embodiments of the present application to facilitate understanding, and they should be considered as merely exemplary.
Accordingly, those of ordinary skill in the art will recognize that various changes and modifications of the embodiments described herein can be made without departing from the scope and spirit of the present application.
Also, in the following description, descriptions of well-known functions and structures are omitted for clarity and conciseness.

[n0019]

It should be noted that, in the absence of conflict, the embodiments and features in the embodiments of the present application may be combined with each other.

The present application will be described in detail below with reference to the accompanying drawings and in combination with embodiments.

[n0020]

FIG. 1 shows an exemplary system architecture 100 to which an embodiment of a system disaster recovery method or a system disaster recovery apparatus of the present application can be applied.

[n0021]

As shown in FIG. 1 , system architecture 100 may include a system 101 and a caller 102 that calls a service provided by the system.
The system 101 may include a controller 1011 , a cluster 1012 , and a cluster 1013 .
The controller 1011 may send control instructions to the cluster 1012 and the cluster 1013 to control the cluster 1012 and the cluster 1013 to perform various operations, such as data synchronization.
One of cluster 1012 and cluster 1013 may be a primary cluster, and the other may be a backup cluster.
The primary cluster and the backup cluster can be converted under certain circumstances. For example, when a cluster fails, the backup cluster can become the primary cluster, and the failed cluster can become the backup cluster when it is restored.
To ensure the normal provision of services, data can be synchronized between clusters in real time, or backed up according to pre-set rules.

[n0022]

The caller 102 may be any electronic device that calls services provided by the system 101 , and may implement various data processing by calling services.

[n0023]

It should be noted that the controller 1011, cluster 1012, cluster 1013 and caller 102 can be hardware or software.
When it is hardware, it can be implemented as a distributed server cluster consisting of multiple servers, or it can be implemented as a single server.
When it is software, it can be implemented as multiple software or software modules (for example, to provide distributed services), or it can be implemented as a single software or software module.
No specific limitation is given here.

[n0024]

It should be noted that the system disaster recovery method provided in the embodiment of the present application is generally executed by the controller 1011 .
Accordingly, the system disaster recovery device is generally arranged in the controller 1011 .

[n0025]

It should be understood that the number of electronic devices in the controller, cluster, and caller in FIG. 1 is merely illustrative.
Depending on the implementation needs, there can be any number of controllers, clusters, and electronic devices in the caller.

[n0026]

Continuing to refer to FIG. 2 , a process 200 of an embodiment of a system disaster recovery method according to the present application is shown.
The system disaster recovery method of this embodiment includes the following steps:

[n0027]

Step 201: In response to determining that a primary cluster in the system fails, determine whether a backup cluster in the system is available.

[n0028]

In this embodiment, the execution subject of the system disaster recovery method (eg, the controller 1011 shown in FIG. 1) can monitor the status of the main cluster in the system in real time.
If a primary cluster failure is detected, it can be detected whether a backup cluster in the system is available.
The primary cluster and the backup cluster can be two clusters with the same configuration.
The backup cluster can synchronize data from the primary cluster in real time to ensure that services can be provided at any time.

[n0029]

The execution subject can detect the status of the primary cluster and the backup cluster in various ways, such as by sending heartbeat packets.

Specifically, the execution subject may send a heartbeat packet to each node in the cluster. If a response message is received within a preset time, the node is considered available.
A cluster is considered available if the number of available nodes is greater than one-half the number of nodes in the cluster.
Similarly, if the number of available nodes is less than or equal to one-half the number of nodes in the cluster, the cluster is considered to be faulty.

[n0030]

Step 202: In response to determining that the backup cluster is available, modify cluster configuration information.

[n0031]

If the execution subject determines that the backup cluster is available, the cluster configuration information can be modified.
Here, the cluster configuration information may include information such as interfaces for calling various services provided by the cluster and addresses of nodes providing various services.
The execution subject can modify the cluster configuration information according to the services that the backup cluster can provide and the interfaces required by the above services.

[n0032]

Step 203: output the modified cluster configuration information to the user of the primary cluster, so that the user can use the backup cluster according to the modified cluster configuration information.

[n0033]

The execution subject can output the modified cluster configuration information to the user of the main cluster.
After receiving the modified cluster configuration information, each user can modify the address information or interface information of the request to use the backup cluster to process the request.

[n0034]

Continuing to refer to FIG. 3 , it shows a schematic diagram of an application scenario of the system disaster recovery method according to the present application.

In the application scenario of FIG. 3 , after detecting a failure of the primary cluster 302 , the controller 301 determines that the backup cluster 303 is available, and can modify the cluster configuration information and send the modified cluster configuration information to the user 304 of the primary cluster 302 .
After receiving the modified cluster configuration information, the user 304 modifies the address of the request, thereby sending the request to the backup cluster 303 .
After receiving the request, the backup cluster 303 processes the request.

[n0035]

The system disaster recovery method provided by the above-mentioned embodiment of the present application can modify the system configuration information when the main cluster fails, and output it to the user who calls the main cluster, so that the user can modify the configuration according to the system configuration information, thereby switching to an available backup cluster, thereby ensuring the high availability of system services.

[n0036]

Continuing to refer to FIG. 4 , it shows a process 400 of another embodiment of the system disaster recovery method according to the present application.
As shown in FIG4 , the method of this embodiment may include the following steps:

[n0037]

Step 401, controlling the backup cluster to synchronize data from the primary cluster in real time.

[n0038]

In this embodiment, the execution entity may send a synchronization instruction to the backup cluster.
After receiving the above synchronization instruction, the backup cluster can synchronize data from the primary cluster in real time.
In this way, data consistency can be guaranteed.

[n0039]

Step 402: Determine whether the main cluster fails according to the number of available nodes in the main cluster, the number of nodes in the main cluster, and a preset ratio threshold.

[n0040]

The execution entity may first determine whether each node in the main cluster is available, and count the number of available nodes.
Whether the main cluster fails is determined based on the number of available nodes in the main cluster, the number of nodes in the main cluster, and a preset ratio threshold.
Specifically, the execution entity may calculate the ratio of the number of available nodes to the number of nodes in the main cluster.
If the above ratio threshold is greater than a preset ratio threshold, it can be determined that the primary cluster is available.
Otherwise, it is considered that the main cluster fails.

[n0041]

It is understandable that the execution entity can use the same method to detect whether the backup cluster is available.

[n0042]

Step 403: in response to determining that the primary cluster fails, output a first alarm message; control the backup cluster to stop synchronizing data from the primary cluster; and determine whether the backup cluster is available.

[n0043]

After determining that the primary cluster fails, the execution subject can perform the following operations: output the first alarm information; control the backup cluster to stop synchronizing data from the primary cluster; and determine whether the backup cluster is available.
Here, the first alarm information is used to remind the technician that the main cluster is unavailable, and the technician can perform fault diagnosis or other processing on the main cluster.
After the primary cluster fails, the primary cluster will not generate correct data. The execution entity can control the backup cluster to stop synchronizing data from the primary cluster.
At the same time, the execution subject can further confirm whether the backup cluster is available.

[n0044]

Step 404: in response to determining that the backup cluster is available, obtaining address information of the backup cluster; and modifying cluster configuration information according to the address information of the backup cluster.

[n0045]

If the backup cluster is available, obtain the address information of the backup cluster. Then, modify the cluster configuration information according to the address information of the backup cluster.
Specifically, the above cluster configuration information includes address information of the cluster, and the execution subject can use the address information of the backup cluster to replace the address information in the cluster configuration information to modify the cluster configuration information.

[n0046]

In some optional implementations of this embodiment, the execution entity may store the address information required by the users of each cluster together (for example, in a fixed electronic device, which becomes a configuration center).
When modifying cluster configuration information, the execution entity can obtain the address information required by each user from the configuration center for modification. For example, user A needs the address information of node a1 in the primary cluster, and user B needs the address information of node b1 in the primary cluster.
Node a1 in the primary cluster corresponds to node a2 in the backup cluster, and node b1 in the primary cluster corresponds to node b2 in the backup cluster.
During modification, the address information in the cluster configuration information of user A may be modified to the address information of node a2 in the backup cluster, and the address information in the cluster configuration information of user B may be modified to the address information of node b2 in the backup cluster.

[n0047]

Step 405: output the modified cluster configuration information to the user of the primary cluster through a preset interface, so that the user can use the backup cluster according to the modified cluster configuration information.

[n0048]

After modifying the cluster configuration information, the execution subject can output the modified cluster configuration information to the user of the main cluster through a preset interface.
In this embodiment, the configuration center may also be provided with an interface for interacting with various users.
The execution subject can directly call the above interface to output the modified cluster configuration information to each user, so that the user can use the backup cluster according to the modified cluster configuration information.

[n0049]

It is understandable that after switching to the backup cluster, the backup cluster can be used as a new primary cluster, and after the failed primary cluster is restored, it can be used as a backup cluster of the new primary cluster.

[n0050]

Step 406: In response to determining that the primary cluster has recovered from the failure, control the primary cluster to synchronize data from the backup cluster.

[n0051]

In this embodiment, if the primary cluster fails and recovers, the execution subject can send a control instruction to the primary cluster to synchronize data from the backup cluster. The synchronization here can be an incremental backup to ensure the consistency of data in the two clusters.

[n0052]

The system disaster recovery method provided by the above-mentioned embodiment of the present application can maintain the consistency of the main cluster and the backup cluster, and can also directly interact with each user of the main cluster through a preset interface, thereby improving the efficiency of cluster configuration information delivery.

[n0053]

Further referring to FIG. 5 , as an implementation of the methods shown in the above figures, the present application provides an embodiment of a system disaster recovery device, which corresponds to the method embodiment shown in FIG. 2 , and can be specifically applied to various electronic devices.

[n0054]

As shown in FIG. 5 , the device 500 for outputting information in this embodiment includes: a state determining unit 501 , an information modifying unit 502 , and an information outputting unit 503 .

[n0055]

The state determination unit 501 is configured to determine whether a backup cluster in the system is available in response to determining that a primary cluster in the system fails.

[n0056]

The information modification unit 502 is configured to modify the cluster configuration information in response to determining that the backup cluster is available.

[n0057]

The information output unit 503 is configured to output the modified cluster configuration information to the user of the primary cluster, so that the user can use the backup cluster according to the modified cluster configuration information.

[n0058]

In some optional implementations of this embodiment, the information modification unit 502 may be further configured to: obtain address information of the backup cluster; and modify the cluster configuration information according to the address information of the backup cluster.

[n0059]

In some optional implementations of this embodiment, the information output unit 503 may be further configured to: output the modified cluster configuration information to a user of the main cluster through a preset interface.

[n0060]

In some optional implementations of this embodiment, the device 500 may further include a status detection unit not shown in Figure 5, which is configured to determine whether the main cluster is faulty based on the number of available nodes in the main cluster, the number of nodes in the main cluster, and a preset ratio threshold.

[n0061]

In some optional implementations of this embodiment, the device 500 may further include an alarm information output unit not shown in Figure 5, which is configured to: output first alarm information in response to determining a primary cluster failure; output second alarm information in response to determining a backup cluster failure.

[n0062]

In some optional implementations of this embodiment, the device 500 may further include a synchronization control unit not shown in Figure 5, which is configured to: control the backup cluster to synchronize data from the main cluster in real time; in response to determining that the main cluster fails, control the backup cluster to stop synchronizing data from the main cluster.

[n0063]

In some optional implementations of this embodiment, the synchronization control unit may be further configured to: in response to determining that the primary cluster has recovered from a failure, control the primary cluster to synchronize data from the backup cluster.

[n0064]

It should be understood that the units 501 to 503 recorded in the system disaster recovery device 500 correspond to the steps in the method described with reference to FIG. 2 . Therefore, the operations and features described above for the system disaster recovery method are also applicable to the device 500 and the units included therein, and will not be repeated here.

[n0065]

According to an embodiment of the present application, the present application also provides an electronic device, a readable storage medium and a computer program product.

[n0066]

FIG. 6 shows a block diagram of an electronic device 600 for executing a system disaster recovery method according to an embodiment of the present application.
Electronic device is intended to refer to various forms of digital computers, such as laptops, desktops, workstations, personal digital assistants, servers, blade servers, mainframes, and other appropriate computers.

Electronic devices may also refer to various forms of mobile devices, such as personal digital assistants, cellular phones, smart phones, wearable devices, and other similar computing devices.
The components shown herein, their connections and relationships, and their functions, are intended merely as examples, and are not intended to limit implementations of the application described and/or claimed herein.

[n0067]

As shown in FIG. 6 , device 600 includes a computing unit 601 that can perform various appropriate actions and processes according to a computer program stored in a read-only memory unit (ROM) 602 or a computer program loaded from a storage unit 608 to a random access memory unit (RAM) 603 .
In the RAM 603, various programs and data necessary for the operation of the device 600 may also be stored.
The calculation unit 601 , the ROM 602 , and the RAM 603 are connected to one another via a bus 604 .
An I/O interface (input/output interface) 605 is also connected to the bus 604 .

[n0068]

Multiple components in the device 600 are connected to the I/O interface 605, including: an input unit 606, such as a keyboard, a mouse, etc.; an output unit 607, such as various types of displays, speakers, etc.; a storage unit 608, such as a disk, an optical disk, etc.; and a communication unit 609, such as a network card, a modem, a wireless communication transceiver, etc.
The communication unit 609 allows the device 600 to exchange information/data with other devices through a computer network such as the Internet and/or various telecommunication networks.

[n0069]

The computing unit 601 may be a variety of general and/or special processing components having processing and computing capabilities.
Some examples of computing unit 601 include, but are not limited to, a central processing unit (CPU), a graphics processing unit (GPU), various dedicated artificial intelligence (AI) computing chips, various computing units that run machine learning model algorithms, a digital signal computing unit (DSP), and any appropriate computing unit, controller, microcontroller, etc.

The computing unit 601 executes the various methods and processes described above, such as the system disaster recovery method.
For example, in some embodiments, the system disaster recovery method may be implemented as a computer software program that is tangibly contained in a machine-readable storage medium, such as the storage unit 608 .
In some embodiments, part or all of the computer program may be loaded and/or installed on the electronic device 600 via the ROM 602 and/or the communication unit 609 .
When the computer program is loaded into the RAM 603 and executed by the computing unit 601 , one or more steps of the system disaster recovery method described above may be performed.
Alternatively, in other embodiments, the computing unit 601 may be configured to execute the system disaster recovery method in any other appropriate manner (for example, by means of firmware).

[n0070]

Various implementations of the systems and techniques described above in this document can be implemented in digital electronic circuit systems, integrated circuit systems, field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), application specific standard products (ASSPs), systems on chips (SOCs), load programmable logic devices (CPLDs), computer hardware, firmware, software, and/or combinations thereof. These various embodiments may include being implemented in one or more computer programs that can be executed and/or interpreted on a programmable system including at least one programmable computing unit, which can be a special purpose or general purpose programmable computing unit that can receive data and instructions from a storage system, at least one input device, and at least one output device, and transmit data and instructions to the storage system, the at least one input device, and the at least one output device.

[n0071]

Program codes for implementing the methods of the present application may be written in any combination of one or more programming languages.
The above program codes can be packaged into a computer program product.
These program codes or computer program products can be provided to a computing unit or controller of a general-purpose computer, a special-purpose computer or other programmable data processing device, so that when the program code is executed by the computing unit 601, the functions/operations specified in the flowchart and/or block diagram are implemented.

The program code may execute entirely on the machine, partly on the machine, as a stand-alone software package, partly on the machine and partly on a remote machine or entirely on the remote machine or server.

[n0072]

In the context of this application, a machine-readable storage medium may be a tangible medium that can contain or store a program for use by or in connection with an instruction execution system, apparatus, or device.
The machine-readable storage medium may be a machine-readable signal storage medium or a machine-readable storage medium.
A machine-readable storage medium may include, but is not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing.
More specific examples of machine-readable storage media would include electrical connections based on one or more wires, a portable computer disk, a hard disk, a random access memory unit (RAM), a read-only memory unit (ROM), an erasable programmable read-only memory unit (EPROM or flash memory unit), optical fibers, a portable compact disk read-only memory unit (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the above.

[n0073]

To provide interaction with a user, the systems and techniques described herein can be implemented on a computer having: a display device (e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor) for displaying information to the user; and a keyboard and pointing device (e.g., a mouse or trackball) through which the user can provide input to the computer.
Other types of devices may also be used to provide interaction with a user; for example, the feedback provided to the user may be any form of sensory feedback (e.g., visual feedback, auditory feedback, or tactile feedback); and input from the user may be received in any form (including acoustic input, voice input, or tactile input).

[n0074]

The systems and techniques described herein may be implemented in a computing system that includes back-end components (e.g., as a data server), or a computing system that includes middleware components (e.g., an application server), or a computing system that includes front-end components (e.g., a user computer with a graphical user interface or a

web browser through which a user can interact with implementations of the systems and techniques described herein), or a computing system that includes any combination of such back-end components, middleware components, or front-end components.
The components of the system can be interconnected by any form or medium of digital data communication (eg, a communication network).
Examples of communication networks include a local area network (LAN), a wide area network (WAN), and the Internet.

[n0075]

A computer system may include clients and servers.
A client and server are generally remote from each other and typically interact through a communication network.
The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.
The server can be a cloud server, also known as a cloud computing server or cloud host, which is a host product in the cloud computing service system. It solves the defects of difficult management and weak business scalability in traditional physical hosts and VPS services ("Virtual Private Server", or "VPS" for short).

[n0076]

It should be understood that various forms of the processes shown above may be used, with steps reordered, added or deleted.
For example, the steps described in this application may be executed in parallel, sequentially, or in different orders, as long as the expected results of the technical solution of this application can be achieved, and this document does not impose any restrictions here.

[n0077]

The above specific implementations do not constitute limitations on the protection scope of this application.
It should be apparent to those skilled in the art that various modifications, combinations, sub-combinations and substitutions may be made depending on design requirements and other factors.
Any modifications, equivalent substitutions and improvements made within the spirit and principles of this application should be included in the protection scope of this application.

Notice

CLAIMS CN112527567A

1.

A system disaster recovery method, comprising:
In response to determining that a primary cluster in the system fails, determining whether a backup cluster in the system is available;
In response to determining that the backup cluster is available, modifying cluster configuration information;
The modified cluster configuration information is output to a user of the primary cluster, so that the user can use the backup cluster according to the modified cluster configuration information.

2.

The method according to claim 1, wherein the modifying cluster configuration information comprises:
Obtaining address information of the backup cluster;
The cluster configuration information is modified according to the address information of the backup cluster.

3.

The method according to claim 1, wherein the step of outputting the modified cluster configuration information to a user of the primary cluster comprises:
The modified cluster configuration information is output to the user of the main cluster through a preset interface.

4.

The method according to claim 1, wherein the method further comprises:
Whether the main cluster fails is determined according to the number of available nodes in the main cluster, the number of nodes in the main cluster, and a preset ratio threshold.

5.

The method according to claim 1, wherein the method further comprises:
In response to determining that the main cluster fails, outputting first alarm information;
In response to determining that the backup cluster fails, second alarm information is output.

6.

The method according to claim 1, wherein the method further comprises:
Control the backup cluster to synchronize data from the primary cluster in real time;
In response to determining that the primary cluster fails, the backup cluster is controlled to stop synchronizing data from the primary cluster.

7.

The method according to claim 6, wherein the method further comprises:
In response to determining that the primary cluster has recovered from the failure, the primary cluster is controlled to synchronize data from the backup cluster.

8.

A system disaster recovery device, comprising:
a state determination unit configured to determine whether a backup cluster in the system is available in response to determining that a primary cluster in the system fails;
an information modification unit, configured to modify cluster configuration information in response to determining that the backup cluster is available;
The information output unit is configured to output the modified cluster configuration information to a user of the primary cluster, so that the user can use the backup cluster according to the modified cluster configuration information.

9.

The apparatus according to claim 8, wherein the information modification unit is further configured to:
Obtaining address information of the backup cluster;

The cluster configuration information is modified according to the address information of the backup cluster.

10.

The device according to claim 8, wherein the information output unit is further configured to:
The modified cluster configuration information is output to the user of the main cluster through a preset interface.

11.

The device according to claim 8, wherein the device further comprises a state detection unit configured to:
Whether the main cluster fails is determined according to the number of available nodes in the main cluster, the number of nodes in the main cluster, and a preset ratio threshold.

12.

The device according to claim 8, wherein the device further comprises an alarm information output unit configured to:
In response to determining that the main cluster fails, outputting first alarm information;
In response to determining that the backup cluster fails, second alarm information is output.

13.

The device according to claim 8, wherein the device further comprises a synchronization control unit configured to:
Control the backup cluster to synchronize data from the primary cluster in real time;
In response to determining that the primary cluster fails, the backup cluster is controlled to stop synchronizing data from the primary cluster.

14.

The apparatus according to claim 13, wherein the synchronization control unit is further configured to:
In response to determining that the primary cluster has recovered from the failure, the primary cluster is controlled to synchronize data from the backup cluster.

15.

A system disaster recovery electronic device, comprising:

at least one computing unit; and
A storage unit communicatively connected to the at least one computing unit; wherein,
The storage unit stores instructions that can be executed by the at least one computing unit, and the instructions are executed by the at least one computing unit to enable the at least one computing unit to perform the method according to any one of claims 1 to 7.

16.

A non-transitory computer-readable storage medium storing computer instructions, wherein the computer instructions are used to cause the computer to execute the method according to any one of claims 1 to 7.

17.

A computer program product comprises a computer program, wherein when the computer program is executed by a computing unit, the computer program implements the method according to any one of claims 1 to 7.