CLAIMS

1. A cluster management method, comprising:

acquiring, in a case where a registration request sent by a target device is received, identity information of the target device from the registration request;

performing identity check on the target device based on the identity information to obtain a check result;

acquiring, in a case where the check result is a check success, node information of the target device from the registration request; and

storing the node information to registration information of a device cluster network, to add the target device to the device cluster network,

wherein after storing the node information to the registration information of the device cluster network, the method further comprises:

querying, in a case where state information reported by the target device is not received within a preset length of time, a temporary departure identifier corresponding to the target device from the registration information;

retaining, in a case where the temporary departure identifier is queried, the node information in the registration information; and/or

deleting, in a case where the temporary departure identifier is not queried, the node information from the registration information, to remove the target device from the device cluster network.

2. The method of claim 1, wherein the identity information comprises attribute information and a digital certificate of the target device, and performing the identity check on the target device based on the identity information to obtain the check result comprises:

performing effectiveness verification on the target device by using the attribute

information to obtain a first verification result;

performing legality verification on the digital certificate to obtain a second verification result; and

performing at least one of following operations:

determining, in a case where both the first verification result and the second verification result are a verification success, that the check result is a check success; or

determining, in a case where either the first verification result or the second verification result is a verification failure, that the check result is a check failure.

3. The method of claim 1, wherein the node information comprises device information and network interface information of the target device, and storing the node information to the registration information of the device cluster network comprises:

searching the network interface information from the registration information; and

performing at least one of following operations:

updating, in a case where the network interface information is found, device information associated with the network interface information in the registration information to the device information; or

newly adding, in a case where the network interface information is not found, the device information and the network interface information to the registration information.

4. The method of claim 1, wherein after storing the node information to the registration information of the device cluster network, the method further comprises:

updating, in a case where state information reported by the target device is received, the node information in the registration information and last connection time of the target device according to the state information.

5. A cluster management apparatus, comprising:

an acquisition module, configured to acquire, in a case where a registration request sent by a target device is received, identity information of the target device from the registration request;

a check module, configured to perform identity check on the target device based on the identity information to obtain a check result;

the acquisition module being further configured to acquire, in a case where the check result is a check success, node information of the target device from the registration request; and

a management module, configured to store the node information to registration information of a device cluster network, to add the target device to the device cluster network,

wherein the management module is further configured to:

query, in a case where state information reported by the target device is not received within a preset length of time, a temporary departure identifier corresponding to the target device from the registration information; and

perform at least one of following operations:

retaining, in a case where the temporary departure identifier is queried, the node information in the registration information; or

deleting, in a case where the temporary departure identifier is not queried, the node information from the registration information, to remove the target device from the device cluster network.

6. The apparatus of claim 5, wherein

the management module is further configured to update, in a case where state information reported by the target device is received, the node information in the registration

information and last connection time of the target device according to the state information.

7. An electronic device, comprising a processor, a memory and a communication bus, wherein

the communication bus is configured to implement connection and communication between the processor and the memory;

the processor, when executing one or more programs stored in the memory, is configured to:

acquire, in a case where a registration request sent by a target device is received, identity information of the target device from the registration request;

perform identity check on the target device based on the identity information to obtain a check result;

acquire, in a case where the check result is a check success, node information of the target device from the registration request; and

store the node information to registration information of a device cluster network, to add the target device to the device cluster network,

wherein the processor is further configured to:

query, in a case where state information reported by the target device is not received within a preset length of time, a temporary departure identifier corresponding to the target device from the registration information; and

perform at least one of following operations:

retaining, in a case where the temporary departure identifier is queried, the node information in the registration information; or

deleting, in a case where the temporary departure identifier is not queried, the node information from the registration information, to remove the target device from the device cluster network.

8. The electronic device of claim 7, wherein the identity information comprises attribute information and a digital certificate of the target device, and the processor is configured to:

perform effectiveness verification on the target device by using the attribute information to obtain a first verification result;

perform legality verification on the digital certificate to obtain a second verification result; and

perform at least one of following operations:

determining, in a case where both the first verification result and the second verification result are a verification success, that the check result is a check success; or

determining, in a case where either the first verification result or the second verification result is a verification failure, that the check result is a check failure.

9. The electronic device of claim 7, wherein the node information comprises device information and network interface information of the target device, and the processor is configured to:

search the network interface information from the registration information; and

perform at least one of following operations:

updating, in a case where the network interface information is found, device information associated with the network interface information in the registration information to the device information; and/or

newly adding, in a case where the network interface information is not found, the device information and the network interface information to the registration information.

10. The electronic device of claim 7, wherein the processor is further configured to:

update, in a case where state information reported by the target device is received, the node information in the registration information and last connection time of the target device according to the state information.

11. A computer-readable storage medium, storing one or more programs, wherein the one or more programs are executable by one or more processors, to:

acquire, in a case where a registration request sent by a target device is received, identity information of the target device from the registration request;

perform identity check on the target device based on the identity information to obtain a check result;

acquire, in a case where the check result is a check success, node information of the target device from the registration request; and

store the node information to registration information of a device cluster network, to add the target device to the device cluster network,

wherein the one or more programs are executable by one or more processors, to:

query, in a case where state information reported by the target device is not received within a preset length of time, a temporary departure identifier corresponding to the target device from the registration information; and

perform at least one of following operations:

retaining, in a case where the temporary departure identifier is queried, the node information in the registration information; or

deleting, in a case where the temporary departure identifier is not queried, the node information from the registration information, to remove the target device from the device cluster network.

12. The storage medium of claim 11, wherein the identity information comprises attribute information and a digital certificate of the target device, and the one or more programs are executable by one or more processors to:

perform effectiveness verification on the target device by using the attribute information to obtain a first verification result;

perform legality verification on the digital certificate to obtain a second verification result; and

perform at least one of following operations:

determine, in a case where both the first verification result and the second verification result are a verification success, that the check result is a check success; or

determine, in a case where either the first verification result or the second verification result is a verification failure, that the check result is a check failure.

13. The storage medium of claim 11, wherein the node information comprises device information and network interface information of the target device, and the one or more programs are executable by one or more processors to:

search the network interface information from the registration information; and

perform at least one of following operations:

updating, in a case where the network interface information is found, device information associated with the network interface information in the registration information to the device information; or

newly adding, in a case where the network interface information is not found, the device information and the network interface information to the registration information.

14. The storage medium of claim 11, wherein the one or more programs are executable by one

or more processors to:

update, in a case where state information reported by the target device is received, the node information in the registration information and last connection time of the target device according to the state information.

15. A computer program, stored in a memory; wherein the computer program, when executed by a processor, implements steps in the method of any one of claims 1 to 4.