SPECIFICATION

METHOD FOR REALIZING CLOUD HOST PERMISSION ASSOCIATION FOR CLOUD HOST AND CLOUD BASTION HOST

TECHNICAL FIELD

The present invention relates to the technical field of cloud computing and information security, and in particular, to a method for realizing cloud host permission association for a cloud host and a cloud bastion host.

BACKGROUND

A cloud host is an important part of cloud computing in infrastructure applications, and is located at the bottom of the industrial chain pyramid of cloud computing, with products derived from a cloud computing platform. The platform integrates three core elements of Internet applications: computing, storage and network, and provides public Internet infrastructure services for users. The cloud host is a virtualization technology similar to a virtual private server (VPS) host. In a VPS, virtualization software such as virtual zone (VZ) or virtual machine (VM) is used to virtualize a plurality of parts similar to independent hosts on one host, so that a standalone host with a plurality of users can be implemented, each part may be used as a separate operating system, with a management method the same as that in the host. With the development of cloud computing of the cloud host, the problem of network security cannot be ignored.

As an important part of a security system of the cloud computing platform, a bastion host plays a key role in security compliance audit in a hybrid cloud environment, and also faces many problems, including: highly heterogeneous and widely distributed infrastructures; and cloud resource management in the case of cloud dynamic resource delivery and autoscaling.

First, construction of the cloud computing platform introduces a large quantity of different types of IT infrastructures, including a conventional physical device, a virtualization platform and a private cloud inside the enterprise, and a public cloud. A current cloud platform uses a multi-organization and multi-tenant mode, resulting in a wide range of IT asset distribution and loose management. A traditional bastion host needs to divide resource permissions based on a cloud computing platform architecture, resulting in high manual maintenance cost.

Second, the cloud computing platform is relatively isolated from the conventional bastion host, making it difficult to associate the tenant of the cloud computing platform with the user of the bastion host. Users usually need to be created on the bastion host based on a permission of an organization tenant account corresponding to the resource of the cloud computing platform, and a

corresponding resource permission needs to be assigned to the users, which requires high manual cost.

In addition, the existing traditional bastion host and the cloud computing platform each use different identity authentication systems. When a permission of the tenant of the cloud computing platform is changed, a permission of the user of the corresponding bastion host cannot be adjusted in time, and configuration needs to be manually adjusted, resulting in poor timeliness. It is difficult to implement permission association of the cloud host resources between the cloud computing platform and the traditional bastion host. The two maintenance systems have manual errors, which further increases the manual cost.

Therefore, in view of the problems of a high threshold and low timeliness of the traditional bastion host, how to resolve the problems that infrastructures of the cloud computing platform are highly heterogeneous and have a disorderly distribution, and isolation between the cloud computing platform and the conventional bastion host makes it difficult to implement permission association or to change permission association, and the problems that the cloud tenants have different permissions on the cloud platform based on their own organizations and workspaces, where the permissions are also different from those of the cloud hosts managed by the cloud tenants, and the traditional bastion host cannot implement permission association with the cloud platform is the technical problem to be solved urgently.

SUMMARY

In view of the problem of a high threshold and low timeliness of the traditional bastion host, how to resolve the problems that infrastructures of a cloud computing platform are highly heterogeneous and have a disorderly distribution, and isolation between the cloud computing platform and the conventional bastion host makes it difficult to implement permission association or to change permission association, and the problems that cloud tenants have different permissions on the cloud platform based on their own organizations and workspaces, where the permissions are also different from those of the cloud hosts managed by the cloud tenants, and the traditional bastion host cannot implement permission association with the cloud platform is the technical problem to be solved urgently. The present invention provides a method for realizing cloud host permission association for a cloud host and a bastion host.

The present invention seeks to protect the following technical solutions.

The present invention provides a method for realizing cloud host permission association for a cloud host and a bastion host, including the following processes:

S1: deploying and integrating an open-source bastion host, specifically, deploying the bastion host on a cloud computing platform through providing open-source of the bastion hosts own open API interface, so that the cloud bastion host is applicable to a cloud computing multi-cloud-tenant and multi-cloud-resource scenario, to implement connection and integration between the cloud computing platform and the cloud bastion host;

S2: managing permission information in a unified manner, specifically, in the cloud bastion host, managing an access authorization relationship and access account information between the cloud computing platform and the cloud bastion host in the unified manner based on the connected cloud computing platform and cloud bastion host, to ensure the usage security of all cloud hosts while realizing secure operation and maintenance;

S3: creating a rule for automatically synchronizing and responding to permission information, specifically, creating, in the cloud bastion host, a rule for automatically synchronizing and responding to the permission information, where when a permission of a cloud tenant is adjusted, an account permission of the cloud bastion host is also automatically responded and synchronously changed, to implement automatic synchronization of the permission information between the cloud computing platform and the cloud bastion host, without manual intervention; and

S4: performing association authorization, specifically, in the bastion host, managing the access authorization relationship and the access account information in the unified manner by obtaining changes of an operation permission and a management permission of a main cloud host. to which a cloud host resource belongs, automatically responding to the rule for automatically synchronizing the permission information, and synchronously adjusting the cloud host resource corresponding to the cloud bastion host, where after the authorization relationship of the cloud host resource is changed, the authorization relationship is automatically synchronized to the cloud bastion host, to implement association authorization between a role and the permission of the cloud tenant and the cloud host resource of the cloud bastion host, and enhance an automatic synchronization capability and the security compliance of the cloud tenant and the cloud host resource.

Further, in step S2, the ensuring usage security of all the cloud hosts while realizing secure operation and maintenance by the cloud bastion host includes: performing all operations on the cloud host resource on the cloud platform based on unified identity authentication and log recording of the cloud bastion host, where control on permissions such as uploading/downloading and copying/pasting can better manage and control a security operation and maintenance risk in a scenario such as remote office, to ensure the usage security of all the cloud hosts.

Further, in step S1, in addition to a function that can be provided by a cloud bastion host system, the cloud bastion host may further implement an effect of integrating the cloud platform and the bastion host, and provide the terminal cloud tenant with a bastion host login capability, which is used as one of cloud platform services, so that the cloud tenant may directly jump to use the cloud bastion host through the cloud platform.

Further, a cloud platform administrator of the cloud tenant can manually synchronize a concerned cloud host resource on a management interface, so that updates of all related basic information, permission information and the like can be synchronized to the cloud bastion host.

Further, in step S4, the role and the permission of the cloud tenant refers to a role and a permission that have been distinguished by the cloud tenant on the cloud platform, and different organizations and workspaces have different roles and permissions.

Preferably, the cloud bastion host uses a distributed architecture, supports multi-room cross-area deployment, supports horizontal extension, and has no amount and concurrency limitations on the cloud host resource.

The present invention further provides an apparatus for realizing cloud host permission association for a cloud host and a bastion host, including:

an open-source bastion host deploying and integrating module, configured to: perform deployment on a cloud computing platform through providing open-source of the bastion hosts own open API interface, so that the cloud bastion host is applicable to a cloud computing multi-cloud-tenant and multi-cloud-resource scenario, to implement connection and integration between the cloud computing platform and the cloud bastion host;

a permission information management module, configured to: in the cloud bastion host, manage an access authorization relationship and access account information between the cloud computing platform and the cloud bastion host in a unified manner based on the connected cloud computing platform and cloud bastion host, to ensure the usage security of all cloud hosts while realizing secure operation and maintenance;

a module for automatically synchronizing and responding to permission information, configured to: automatically synchronize and respond to the permission information in the cloud bastion host, where when a permission of a cloud tenant is adjusted, an account permission of the cloud bastion host is also automatically responded and synchronously changed, to implement automatic synchronization of the permission information between the cloud computing platform and the cloud bastion host, without manual intervention; and

an association authorization module, configured to: in the bastion host, manage the access authorization relationship and the access account information in the unified manner by obtaining changes of an operation permission and a management permission of a main cloud host, to which a cloud host resource belongs, automatically respond to the rule for automatically synchronizing permission information, and synchronously adjust the cloud host resource corresponding to the cloud bastion host, where after the authorization relationship of the cloud host resource is changed, the authorization relationship is automatically synchronized to the cloud bastion host, to implement association authorization between the role and the permission of the cloud tenant and the cloud host resource of the cloud bastion host, and enhance an automatic synchronization capability and the security compliance of the cloud tenant and the cloud host resource.

The present invention further provides an electronic apparatus, where the apparatus includes a memory and a processor, the memory stores a configuration program that may run, on the processor, the apparatus for realizing cloud host permission association for a cloud host and a bastion host; and when the configuration program is executed by the processor, the method for realizing cloud host permission association for the cloud host and the bastion host may be implemented.

The present invention further provides a computer-readable storage medium, characterized in that the computer-readable storage medium stores a configuration program of the apparatus for realizing cloud host permission association for the cloud host and the bastion host, and the configuration program may be executed by one or more processors, to implement the method for realizing cloud host permission association for the cloud host and the bastion host.

Compared with the conventional technology, the present invention has the following advantages.

The present invention implements synchronization and updates of permissions of a cloud host in a cloud bastion host by different cloud tenants within their current permission ranges under unified management of a cloud platform. After a permission of one cloud tenant is changed, the cloud tenant may directly log in to the cloud bastion host through the cloud platform.

Through seamless connection between the cloud computing platform and the cloud bastion host, unified identity authentication between the cloud computing platform and the cloud bastion host implements automatic synchronization of the cloud host resource information and the permission information between the cloud computing platform and the cloud bastion host and association of user permissions between the cloud computing platform and the cloud bastion host.

When the permission of the tenant of the cloud platform is adjusted, the account permission of the cloud bastion host is changed synchronously, without manual intervention.

Association authorization is performed between the role and the permission of the tenant of the cloud computing platform and the cloud host asset of the cloud bastion host. When the cloud host resource of the tenant of the cloud platform is newly added, deleted or changed, the cloud host resource of the corresponding cloud bastion host is adjusted synchronously, and association authorization is performed based on the permission of the tenant of the cloud computing platform.

Through connection between the cloud computing platform and the cloud bastion host, a same identity authentication system is used to implement association authorization between the cloud computing platform and the cloud bastion host. This not only reduces operation and maintenance costs of manually maintaining two systems, but also resolves the problems of manual errors and poor timeliness that may be caused by manual maintenance.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram showing steps of a method for realizing cloud host permission association for a cloud host and a bastion host according to the present invention.

FIG. 2 is a diagram of configuration program modules for realizing cloud host permission association for a cloud host and a bastion host according to the present invention.

FIG. 3 is an implementation flowchart of a method for realizing cloud host permission association for a cloud host and a bastion host according to the present invention.

DETAILED DESCRIPTION

To enable a person skilled in the art to better understand the solutions of the present invention, the following clearly and completely describes the technical solutions in the embodiments of the present invention with reference to the accompanying drawings in the embodiments of the present invention. It is clear that, the described embodiments are some rather than all of the embodiments of the present invention. All other embodiments obtained by a person of ordinary skill in the art based on the embodiments of the present invention without creative efforts shall fall within the protection scope of the present invention.

It needs to be noted that the terms such as "first" and "second" in the specification, claims, and the foregoing accompanying drawings of the present invention are only used to distinguish between similar objects, but are not used to describe a specific order or time sequence. It should be understood that the data thus used are interchangeable in appropriate circumstances and that the embodiments of the present invention described herein can be implemented in a sequence other than

those illustrated or described. In addition, the terms "include", "comprise", and any variation of such terms are intended to cover a non-exclusive inclusion. For example, a process, method, system, product, or device that includes a series of steps or units not only includes those steps or units specified expressly, but also includes other steps or units that are not specified expressly or are inherent to the process, method, product, or device.

The present invention uses the following solutions.

Through connection and function development between a cloud computing platform and an open-source bastion host, automatic synchronization of cloud host resource information and permission information between the cloud computing platform and a cloud bastion host is completed. In addition, through unified identity and permission management, account permission association between a tenant of the cloud computing platform and a user of the cloud bastion host is implemented.

Through association authorization performed on a role and a permission of the tenant of the cloud computing platform and a cloud host resource of the cloud bastion host, an automatic synchronization capability and the security compliance of the cloud tenant and a cloud asset are enhanced.

The cloud computing platform and the cloud bastion host use one identity authentication system to manage an access authorization relationship and access account information in a unified manner and implement seamless connection, resource management and comprehensive audit management between the cloud computing platform and the bastion host.

To make advantages of the technical solutions of the present invention clearer, the following describes the present invention in detail with reference to the accompanying drawings and the embodiments.

FIG. 1 is a diagram showing steps of a method for realizing cloud host permission association for a cloud host and a bastion host according to the present invention.

As shown in FIG. 1, the present invention provides a method for realizing cloud host permission association for a cloud host and a bastion host according to the present invention, including the following steps:

Step S1: Deploying and integrating an open-source bastion host, meaning that the bastion host is deployed on a cloud computing platform through providing open-source of the bastion hosts own open API interface, so that the cloud bastion host is applicable to a cloud computing multi-cloud-tenant and multi-cloud-resource scenario, to implement connection and integration

between the cloud computing platform and the cloud bastion host. In this embodiment, the deploying and integrating the open-source bastion host includes: performing cloud-based construction of a module applicable to the cloud computing multi-cloud-tenant and multi-cloud-resource scenario in the bastion host by using the open-source bastion host and the cloud computing platform.

In addition to a function that may be provided by a cloud bastion host system, the cloud bastion host may further implement an effect of integrating the cloud platform and the bastion host, and provide the terminal cloud tenant with a bastion host login capability, which is used as one of cloud platform services, so that the cloud tenant may directly jump to use the cloud bastion host through the cloud platform. This implements synchronization and updates of permissions of a cloud host in a cloud bastion host by different cloud tenants within their current permission ranges under unified management of a cloud platform. After a permission of one cloud tenant is changed, the cloud tenant may directly log in to the cloud bastion host through the cloud platform.

The cloud bastion host uses a distributed architecture, supports multi-room cross-area deployment, supports horizontal extension, and has no amount and concurrency limitations on the cloud host resource. It should be noted that the open-source bastion host described in the present invention includes, but is not limited to, an open-source bastion host product in the industry, for example, a Jumpserver.

In this embodiment, a cloud platform administrator of the cloud tenant may manually synchronize a concerned cloud host resource on a management interface, so that updates of all related basic information, permission information and the like can be synchronized to the cloud bastion host.

Step S2: Managing permission information in a unified manner, meaning that in the cloud bastion host, an access authorization relationship and access account information between the cloud computing platform and the cloud bastion host are managed in the unified manner based on the connected cloud computing platform and cloud bastion host, to ensure the usage security of all cloud hosts while realizing secure operation and maintenance.

In this embodiment, the ensuring the usage security of all the cloud hosts while realizing secure operation and maintenance by the cloud bastion host includes: performing all operations on the cloud host resource on the cloud platform based on unified identity authentication and log recording of the cloud bastion host, where control on permissions such as uploading/downloading and copying/pasting can better manage and control a security operation and maintenance risk in a

scenario such as remote office, to ensure the usage security of all the cloud hosts.

Step S3: Creating a rule for automatically synchronizing and responding to permission information: in the cloud bastion host, a rule for automatically synchronizing and responding to the permission information is created, where when a permission of a cloud tenant is adjusted, an account permission of the cloud bastion host is also automatically responded and synchronously changed, to implement automatic synchronization of the permission information between the cloud computing platform and the cloud bastion host, without manual intervention.

Step S4: Performing association authorization, meaning that in the bastion host, the ccess authorization relationship and the access account information are managed in the unified manner by obtaining changes of an operation permission and a management permission of a main cloud host, to which a cloud host resource belongs; and in automatic response to the rule for automatically synchronizing permission information, the cloud host resource corresponding to the cloud bastion host is synchronously adjusted, where after the resource authorization relationship of the cloud host is changed, the resource authorization relationship is automatically synchronized to the cloud bastion host, to implement association authorization between a role and the permission of the cloud tenant and the cloud host resource of the cloud bastion host, and enhance an automatic synchronization capability and the security compliance of the cloud tenant and the cloud host resource.

In this embodiment, the security compliance, for example, a length of a cloud host account password of the cloud computing resource, a random combination, a periodic update and modification, a cloud tenant who does not know a password of a cloud resource super administrator but may perform an operation and record a trace, and a traceability requirement are considered.

In this embodiment, the role and the permission of the cloud tenant refers to the role and the permission that have been distinguished by the cloud tenant on the cloud platform, and different organizations and workspaces have different roles and permission.

When the cloud host resource of the tenant of the cloud platform is newly added, deleted, or changed, the cloud host resource of the corresponding cloud bastion host is adjusted synchronously, and association authorization is performed based on the permission of the tenant of the cloud computing platform.

During actual application, when a cloud host resource is newly added, for example, a cloud tenant A of the cloud computing platform applies for a new cloud host resource B, the cloud computing platform initiates, based on its own algorithm, a password c that meets a compliance

requirement. In this case, if a traditional bastion host cannot complete identification and management (which require manual operations), when a cloud bastion host D in the method is used, association synchronization of the newly added cloud resource, related basic information, and the password c may be completed; and meanwhile, the cloud tenant A has permissions of different cloud accounts for the cloud resource B based on a permission of the cloud tenant A of the cloud platform, and the cloud bastion host D may also complete corresponding association synchronization to ensure the bastion host capability within the permission range of the cloud tenant.

In this embodiment, the cloud bastion host connected to the cloud computing platform uses a same identity authentication system as the cloud computing platform, to automatically respond to a permission synchronization rule after unified management of permission information, and automatically implement association authorization between the cloud computing platform and the cloud bastion host, without manual intervention in the whose process. This not only reduces operation and maintenance costs of manually maintaining two systems, but also resolves the problems of manual errors and poor timeliness that may be caused by manual maintenance.

In this embodiment, the permission association method is further implemented at a back end of the cloud platform, and no operation is required by a user. A cloud platform administrator may manually synchronize the concerned cloud host asset on the management interface. In this way, updates of all the related basic information, the permission information and the like can be synchronized to the bastion host.

FIG. 2 is a diagram of configuration program modules for realizing cloud host permission association for a cloud host and a bastion host according to the present invention. As shown in FIG. 2, the following modules are included.

An open-source bastion host deploying and integrating module 101 is configured to: perform deployment on a cloud computing platform through providing open-source of the bastion hosts own open API interface, so that the cloud bastion host is applicable to a cloud computing multi-cloud-tenant and multi-cloud-resource scenario, to implement connection and integration between the cloud computing platform and the cloud bastion host. In this embodiment, the open-source bastion host deploying and integrating module 101 is to perform cloudbased construction of a functional module applicable to the cloud computing multi-cloud-tenant and multi-cloud-resource scenario in the bastion host by using the open-source bastion host and the cloud computing platform.

A permission information management module 102 is configured to: in the cloud bastion host, manage an access authorization relationship and access account information between the cloud computing platform and the cloud bastion host in a unified manner based on the connected cloud computing platform and cloud bastion host, to ensure the usage security of all cloud hosts while realizing secure operation and maintenance;

A module 103 for automatically synchronizing and responding to permission information is configured to: automatically synchronize and respond to the permission information in the cloud bastion host, where when a permission of a cloud tenant is adjusted, an account permission of the cloud bastion host is also automatically responded and synchronously changed, to implement automatic synchronization of permission information between the cloud computing platform and the cloud bastion host, without manual intervention.

A association authorization module 104 is configured to: in the bastion host, manage the access authorization relationship and the access account information in the unified manner by obtaining changes of an operation permission and a management permission of a main cloud host, to which a cloud host resource belongs, automatically respond to the rule for automatically synchronizing permission information, and synchronously adjust the cloud host resource corresponding to the cloud bastion host, where after the authorization relationship of the cloud host resource is changed, the authorization relationship is automatically synchronized to the cloud bastion host, to implement association authorization between a role and the permission of the cloud tenant and the cloud host resource of the cloud bastion host, and enhance an automatic synchronization capability and the security compliance of the cloud tenant and the cloud host resource.

FIG. 3 is an implementation flowchart of a method for realizing cloud host permission association for a cloud host and a bastion host according to the present invention. A cloud tenant logs in to a cloud platform to access the workspace of the cloud tenant. When the cloud tenant jumps to a corresponding cloud host through a bastion host, if the cloud tenant has the permission, the cloud tenant directly logs in to the cloud host; or if the cloud tenant does not have the permission, the system returns to a login page or notifies the cloud tenant that the cloud tenant does not have the permission to log in to the cloud host.

In the foregoing process of jumping to the corresponding cloud host through the bastion host, in the cloud computing platform, the bastion host has been deployed on the cloud computing platform through providing open-source of the bastion hosts own open API interface, so that the cloud bastion host IS applicable to a cloud computing multi-cloud-tenant and multi-cloud-resource

scenario, to implement connection and integration between the cloud computing platform and the cloud bastion host and use the same identity authentication system. Therefore, the permission of the cloud tenant may be (has been granted to the cloud platform) changed or replaced through the cloud computing platform.

When the cloud host resource of the tenant of the cloud platform is newly added, deleted, or changed, changed cloud assets, permission of the cloud tenant and permission of the cloud host are synchronized to the corresponding cloud asset information, permission of the cloud tenant, and permission information of the cloud host. A developed association authorization module 104 is configured to: in the bastion host, manage the access authorization relationship and the access account information in the unified manner by obtaining the changes of the operation permission and the management permission of the main cloud host, to which a cloud host resource belongs, automatically respond to the rule for automatically synchronizing permission information, and synchronously adjust the cloud host resource corresponding to the cloud bastion host, where after the authorization relationship of the cloud host resource is changed, the authorization relationship is automatically synchronized to the cloud bastion host, to implement, in a normal case, association authorization between the role and the permission of the cloud tenant and the cloud host resource of the cloud bastion host, the cloud tenant can log in to the cloud host through the bastion host, and enhance an automatic synchronization capability and the security compliance of the cloud tenant and the cloud host resource. The association authorization process does not require manual operations. This not only reduces the operation and maintenance costs of manually maintaining two systems, but also resolves the problems of manual errors and poor timeliness that may be caused by manual maintenance.

It should be further noted that, in a case of login exception or failure, the security compliance needs to be considered. For example, to meet the security compliance and the traceability requirement, a length of a cloud host account password of the cloud computing resource, a random combination, a periodic update and modification, and a cloud tenant who does not know a password of a cloud resource super administrator but can perform an operation and record a trace are used for security assurance. The exception analysis function or security compliance rule claimed in the present invention is not limited to the foregoing process, but should also include common cases such as exception analysis of the login permission in the art.

The present invention further provides an electronic apparatus, where the apparatus includes a memory and a processor, the memory stores a configuration program that may run the apparatus in

this embodiment on the processor, and when the configuration program is executed by the processor, the method for realizing cloud host permission association for a cloud host and a bastion host in this embodiment may be implemented.

The present invention further provides a computer-readable storage medium, where the computer-readable storage medium stores a configuration program of the apparatus in this embodiment, and the configuration program may be executed by one or more processors, to implement the method for realizing cloud host permission association for the cloud host and the bastion host in this embodiment.

The foregoing descriptions are preferred implementations of the present invention. It should be noted that for a person of ordinary skill in the art, several improvements and modifications may further be made without departing from the principle of the present invention. These improvements and modifications should also be deemed as falling within the protection scope of the present invention.

CLAIMS

What is claimed is:

1. A method for realizing cloud host permission association for a cloud host and a bastion host, comprising the following processes:

S1: deploying and integrating an open-source bastion host, deploying the bastion host on a cloud computing platform through providing open-source of a bastion hosts own open API interface,so that the cloud bastion host is applicable to a cloud computing multi-cloud-tenant and multi-cloud-resource scenario, to implement connection and integration between the cloud computing platform and the cloud bastion host;

S2: managing permission information in a unified manner, based on the connected cloud computing platform and cloud bastion host, in the cloud bastion host, managing an access authorization relationship and access account information between the cloud computing platform and the cloud bastion host in the unified manner, to ensure the usage security of all cloud hosts while realizing secure operation and maintenance;

S3: creating a rule for automatically synchronizing and responding to permission information, creating, in the cloud bastion host, the rule for automatically synchronizing and responding to the permission information, wherein when a permission of a cloud tenant is adjusted, an account permission of the cloud bastion host is also automatically responded and synchronously changed, to implement automatic synchronization of the permission information between the cloud computing platform and the cloud bastion host, without manual intervention; and

S4: performing association authorization, in the bastion host, managing the access authorization relationship and the access account information in the unified manner by obtaining changes of an operation permission and a management permission of a main cloud host, to which a cloud host resource belongs, automatically responding to the rule for automatically synchronizing the permission information, and synchronously adjusting the cloud host resource corresponding to the cloud bastion host, wherein after the authorization relationship of the cloud host resource is changed, the authorization relationship may be automatically synchronized to the cloud bastion host, to implement association authorization between a role and the permission of the cloud tenant and the cloud host resource of the cloud bastion host, and enhance an automatic synchronization capability and the security compliance of the cloud tenant and the cloud host resource.

2. The method for cloud host permission association according to claim 1, wherein in step S2, the ensuring the usage security of all the cloud hosts while realizing secure operation and maintenance by the cloud bastion host comprises: performing all operations on the cloud host resource on the cloud platform based on unified identity authentication and log recording of the cloud bastion host, wherein control on permissions such as uploading/downloading and copying/pasting can better manage and control a security operation and maintenance risk in a scenario such as remote office, to ensure the usage security of all the cloud hosts.

3. The method for cloud host permission association according to claim 1, wherein in step S1, in addition to a function that may be provided by a cloud bastion host system, the cloud bastion host may further implement an effect of integrating the cloud platform and the bastion host, and provide the terminal cloud tenant with a bastion host login capability, which is used as one of cloud platform services, so that the cloud tenant may directly jump to use the cloud bastion host through the cloud platform.

4. The method for cloud host permission association according to claim 1, wherein

a cloud platform administrator of the cloud tenant may manually synchronize a concerned cloud host resource on a management interface, due to which, updates of all related basic information, permission information and the like may be synchronized to the cloud bastion host.

5. The method for cloud host permission association according to claim 1, wherein

in step S4, the role and the permission of the cloud tenant refers to a role and a permission that have been distinguished by the cloud tenant on the cloud platform, and different organizations and workspaces have different roles and permissions.

6. The method for cloud host permission association according to claim 1, wherein

the cloud bastion host uses a distributed architecture, supports multi-room cross-area deployment, supports horizontal extension, and has no amount and concurrency limitations on the cloud host resource.

7. An apparatus for realizing cloud host permission association for a cloud host and a bastion host, comprising:

an open-source bastion host deploying and integrating module, configured to perform deployment on a cloud computing platform through providing open-source of the bastion hosts own open API interface, so that the cloud bastion host is applicable to a cloud

computing multi-cloud-tenant and multi-cloud-resource scenario, to implement connection and integration between the cloud computing platform and the cloud bastion host;

a permission information management module, configured to: in the cloud bastion host, manage an access authorization relationship and access account information between the cloud computing platform and the cloud bastion host in a unified manner based on the connected cloud computing platform and cloud bastion host, to ensure the usage security of all cloud hosts while realizing secure operation and maintenance;

a module for automatically synchronizing and responding to permission information, configured to automatically synchronize and respond to the permission information in the cloud bastion host, wherein when the permission of the cloud tenant is adjusted, an account permission of the cloud bastion host is also automatically responded and synchronously changed, to implement automatic synchronization of the permission information between the cloud computing platform and the cloud bastion host, without manual intervention; and

an association authorization module, configured to: in the bastion host, manage the access authorization relationship and the access account information in a unified manner by obtaining changes of an operation permission and a management permission of a main cloud host, to which a cloud host resource belongs, automatically respond to the rule for automatically synchronizing the permission information, and synchronously adjust the cloud host resource corresponding to the cloud bastion host, wherein after the authorization relationship of the cloud host resource is changed, the authorization relationship is automatically synchronized to the cloud bastion host, to implement association authorization between a role and the permission of the cloud tenant and the cloud host resource of the cloud bastion host, and enhance an automatic synchronization capability and the security compliance of the cloud tenant and the cloud host resource.

8. An electronic apparatus, comprising a memory and a processor, the memory stores a configuration program that can run the apparatus according to claim 7 on the processor, and when the configuration program is executed by the processor, the method for realizing cloud host permission association for the cloud host and the bastion host according to any one of claims 1 to 6 may be implemented.

9. A computer-readable storage medium, wherein the computer-readable storage medium stores a configuration program of the apparatus according to claim 7, and the configuration program may be executed by one or more processors, to implement the

method for realizing cloud host permission association for the cloud host and the bastion host according to any one of claims 1 to 6.