

SPECIFICATION

METHOD FOR IMPLEMENTING AUTOMATIC PASSWORD CHANGE HAVING FAULT TOLERANCE MECHANISM FOR CLOUD HOST AND CLOUD BASTION HOST

TECHNICAL FIELD

The present invention relates to the field of cloud computing and information security technologies, and specifically, to a method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts.

BACKGROUND

Cloud hosts are important part of cloud computing in infrastructure applications, and are 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 hosts are a virtualization technology similar to a VPS host. In a VPS, virtualization software such as VZ or VM is used to virtualize multiple parts similar to independent hosts on one host, so that a standalone host with multiple users can be implemented, each part may be used as a separate operating system, and a management method is the same as that in the host. With the development of cloud computing of the cloud hosts, a problem of network security cannot be ignored.

As an important part of a security structure of a 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; an ever-growing scale of cloud resources in a hybrid cloud, requiring the bastion host to have sufficient scalability; and cloud resource management and automatic password changing in the case of cloud dynamic resource delivery and autoscaling.

Due to the conventional physical equipment, virtualization platforms, private clouds, and public clouds inside enterprises, construction of the cloud computing platform has introduced a large number of different types of IT infrastructures. To reduce the difficulty of platform resource management and adapt well to an API interface of the cloud computing platform, the bastion host is required to have good adaptability and flexibility in asset access and management. In addition, a current cloud computing platform has multiple enterprises, multiple organizations, and multiple tenants, resulting in a wide range of IT asset distribution and loose management. An operation and

maintenance security audit system built based on the bastion host needs to provide a multi-level authorization and management structure to adapt to a current IT management mode.

The infrastructures are highly heterogeneous and widely distributed, and manual costs for maintaining information such as the password are high. The construction of the cloud computing platform has introduced a large number of different types of IT infrastructures, including conventional physical bare-metal equipment, virtualization resources for cloud computing, and the like inside enterprises. A conventional bastion host does not have good adaptability and flexibility in asset access and management. In a conventional mode, addition, deletion, modification, and the like of cloud host account require successive manual configuration on both cloud resources and the bastion host, leading to high manual maintenance costs and insufficient accuracy and real-time performance.

Due to isolation between a cloud computing platform and a conventional bastion host, it is difficult to implement real-time linked automatic password changing. The cloud computing platform is relatively isolated from the conventional bastion host, making it difficult to link a tenant of the cloud computing platform and a user of the bastion host. It is usually necessary to manually synchronize and maintain resources of the cloud computing platform and resources of the bastion host. Due to the isolation between the conventional bastion host and the cloud computing platform, it is difficult for the cloud computing platform to perform policy-based periodic automatic password changing through the cloud computing platform.

The cloud resource management in the case of cloud dynamic resource delivery and autoscaling is difficult, and the automatic password changing is unstable. Due to the flexibility of dynamic delivery and autoscaling of cloud resources, changes in resources and information maintenance usually require manual maintenance, leading to poor timeliness. Consequently, a bastion host often encounters a use abnormality due to problems such as untimely information maintenance and incorrect information maintenance, and there are unstable factors in the automatic password changing.

Therefore, how to solve problems that infrastructures of a cloud computing platform are highly heterogeneous and have a disorderly distribution, the isolation between the cloud computing platform and a conventional bastion host makes it difficult to implement automatic password changing, and even if it is implemented, there are some problems such as automatic secret change instability and like problems, which is an urgent technical problem to be solved at present..

SUMMARY

To solve problems that infrastructures of a cloud computing platform are highly heterogeneous

and have a disorderly distribution, the isolation between the cloud computing platform and a conventional bastion host makes it difficult to implement automatic password changing, and even if it is implemented, there are some problems such as automatic secret change instability and like problems. A method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts is developed in the present invention, may complete cloud asset information automatic synchronization between the cloud computing platform and the cloud bastion hosts on the cloud computing platform, and may deliver a password policy by using the cloud computing platform, implementing automatic password changing for the cloud asset information in the cloud computing platform. According to the method, under universal management of the cloud platform, when random password changing for cloud asset information in all cloud computing platforms is completed, the information is synchronized with the cloud bastion hosts, and after automatic password changing, a cloud tenant can directly log in to the cloud bastion hosts by using the cloud platform.

The present invention seeks to protect the following technical solutions.

Through a connection to an api interface of an open-source cloud bastion hosts and with the development of functions, a cloud computing platform completes cloud asset information automatic synchronization between the cloud computing platform and cloud bastion hosts on the cloud computing platform, implementing a seamless connection between the cloud computing platform and the cloud bastion hosts. It is no longer necessary to manually maintain information of two systems. The cloud asset information in the cloud computing platform only needs to be maintained on the cloud computing platform.

In the cloud computing platform, an automatic password changing technology for cloud resources is developed by using an independently developed cloud bastion host verification module and using a cloud computing service arrangement technology, so that a password changing scheme for the cloud asset information in the cloud computing platform may be directly set on the cloud computing platform, to complete automatic password changing and information synchronization through a connection between the cloud computing platform and the open-source cloud bastion hosts.

An automatic password changing fault tolerance mechanism is added to the cloud computing platform to improve the stability of automatic password changing, support policy-based periodic batch password changing, enlarge a password difference among different systems, improve the complexity to satisfy a management requirement, and satisfy requirements for cloud resource security compliance in different service scenarios.

Specifically:

The present invention provides a method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts, where the method specifically

includes the following steps:

S1. deploying and fusing open-source cloud bastion hosts: constructing cloud bastion hosts applicable to a cloud service scenario on a cloud computing platform by using their own open api interfaces of open-source cloud bastion hosts, implement a connection between the cloud computing platform and the cloud bastion hosts, and implement universal management and maintenance of cloud asset information in the cloud computing platform and cloud asset information in the cloud bastion hosts on the cloud computing platform; and simultaneously establishing cloud bastion host verification module on the connected cloud computing platform, to verify and ensure , in a multi-cloud heterogeneous environment, accuracy of the cloud asset information in the cloud computing platform synchronized between the cloud computing platform and the cloud bastion hosts, and ensure that an automatic password changing scheme can be normally performed;

S2. establishing a fault tolerance mechanism response rule: establishing a fault tolerance mechanism response rule added to the cloud computing platform, to enlarge a password difference among different systems, and to improve stability of automatic password changing, where the fault tolerance mechanism is an automatic password changing fault tolerance mechanism added when the cloud bastion host verification module is established on the cloud computing platform;

S3. establishing a response rule for real-time synchronization of the cloud asset information in the cloud computing platform: establishing a real-time response rule for the cloud asset information in the cloud computing platform in service scenarios such as dynamic delivery and autoscaling for the cloud asset information in the cloud computing platform, implementing real-time automatic synchronization related to the cloud asset information in the cloud computing platform and in the cloud bastion hosts on the cloud computing platform;

S4. obtaining a password changing policy: obtaining a scheduled task from the cloud computing platform for automatic password changing and self-defining, and determining a password changing policy according to the scheduled task; and

S5. performing automatic password changing: after the automatic password changing policy is obtained, automatically invoking, in the cloud computing platform, the cloud computing platform and the cloud bastion hosts that are connected in step S1, to complete arrangement of the automatic password changing policy for the cloud asset information in the cloud computing platform; automatically responding to the fault tolerance mechanism and the cloud bastion host verification module in step S2, and performing periodic automatic verification and performing batch password changing by using the cloud bastion hosts according to the automatic password changing policy; and synchronizing a result of automatic execution from the cloud bastion hosts to the cloud computing platform by performing step S3, where the result takes effect in a corresponding cloud hosts.

Further, in step S1, the cloud bastion hosts uses a distributed architecture, supports multi-room cross-area deployment, supports horizontal scaling, and has no amount and concurrency limitations on the cloud asset information in the cloud computing platform;

the cloud asset information in the cloud computing platform includes: basic information such as an ip and a port of the cloud hosts, operation permission information of a cloud tenant, and cloud resource account information of a plurality of accounts such as username and password information of an administrator user/a non-administrator user in resources of the cloud hosts; and

the cloud bastion hosts is provided to the cloud tenants as one of services provided by the cloud computing platform, and the cloud tenants can directly jump by using the cloud computing platform to use the cloud bastion hosts.

Further, in step S1, the cloud bastion host verification module is used by the cloud computing platform to periodically and automatically complete a verification function and/or used by the cloud tenants to manually complete the verification function, to complete verification related to cloud asset information in the cloud hosts in the cloud computing platform by using an automation technology, verify correctness of the cloud asset information in an automatic remote login mode, simultaneously perform verification with the cloud bastion hosts, to ensure that the cloud asset information in the cloud platform is consistent with that in the cloud bastion, and when a verification result is that the information is consistent, initiate verification.

Further, in step S2, the automatic password changing fault tolerance mechanism includes: during execution of an automatic password changing task, controlling to synchronously perform a password verification function one by one, after the password changing is automatically completed, recording a previous password, and then recording a newly changed password together; next, attempting automatic verification on a new password of the cloud hosts, and if the verification fails, rolling back this task of the cloud hosts, to ensure that the old password can be used to log in; terminating all automatic password changing tasks, where manual intervention is required to choose to skip or continue; and if the verification succeeds, continuing to perform a next task.

Further, in step S3, the service scenario such as dynamic delivery and autoscaling includes: dynamic scaling of the resources of the cloud hosts, where a newly scaled cloud hosts has an independent account and password, and the independent account and password are synchronized with the cloud bastion hosts, to ensure operability of resources of the newly scaled cloud hosts.

Further, in step S4, the scheduled task obtained from the cloud computing platform for automatic password changing and self-defining includes: a start time, a list of involved cloud hosts, users of the involved cloud hosts, and the like.

The present invention further provides a device of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts, including:

an open-source cloud bastion host deployment and fusion module, configured to: construct

cloud bastion hosts applicable to a cloud service scenario on a cloud computing platform by using their own open api interfaces of open-source cloud bastion hosts, implement a connection between the cloud computing platform and the cloud bastion hosts, and implement universal management and maintenance of cloud asset information in the cloud computing platform and cloud asset information in the cloud bastion hosts on the cloud computing platform; and simultaneously establish cloud bastion host verification module on the connected cloud computing platform, to verify and ensure , in a multi-cloud heterogeneous environment, accuracy of the cloud asset information in the cloud computing platform synchronized between the cloud computing platform and the cloud bastion hosts, and ensure that an automatic password changing scheme can be normally performed;

a fault tolerance mechanism response module, configured to: automatically respond to a fault tolerance mechanism rule, to enlarge a password difference among different systems, and to improve stability of automatic password changing, where the fault tolerance mechanism is an automatic password changing fault tolerance mechanism added when the cloud bastion host verification module is established on the cloud computing platform;

a response module for real-time synchronization of cloud asset information in a cloud computing platform, configured to: automatically respond to a real-time synchronization rule for the cloud asset information in the cloud computing platform in a service scenario such as dynamic delivery and autoscaling for the cloud asset information in the cloud computing platform, implementing real-time automatic synchronization related to the cloud asset information in the cloud computing platform and in the cloud bastion hosts on the cloud computing platform;

a password changing policy obtaining module, configured to: obtain a scheduled task from the cloud computing platform for automatic password changing and self-defining, and determine a password changing policy according to the scheduled task; and

an automatic password changing execution module, configured to: after the automatic password changing policy is obtained, automatically invoke, in the cloud computing platform, the cloud computing platform and the cloud bastion hosts that are connected by the open-source cloud bastion hosts deployment and fusion module, to complete arrangement of the automatic password changing policy for the cloud asset information in the cloud computing platform; automatically respond to the fault tolerance mechanism and the cloud bastion host verification module in the fault tolerance mechanism response module, and perform periodic automatic verification and perform batch password changing by using the cloud bastion hosts according to the automatic password changing policy; and synchronize a result of automatic execution from the cloud bastion hosts to the cloud computing platform by using the response module for real-time synchronization of cloud asset information in a cloud computing platform, where the result takes effect in a corresponding cloud hosts.

Further, the password changing policy obtaining module further includes:

a display submodule, configured to display an interface of a module specially configured to perform an automatic password changing task of the cloud hosts in the cloud computing platform, so that a timing task of customizing automatic password changing that needs to be started can be provided to a user; and

a self-defining password changing policy submodule, configured to enable a cloud tenant to directly configure a cloud resource password changing scheme by using the cloud computing platform, to obtain a self-defined automatic password changing policy after the configuration is completed.

The present invention further includes an electronic device, where the device includes a memory and a processor, the memory stores a configuration program that can run, on the processor, the device of implementing an automatic password changing technology for cloud hosts and cloud bastion hosts, and the configuration program, when being executed by the processor, can implement the method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts in the present invention.

The present invention further includes a computer-readable storage medium, where the computer-readable storage medium stores a configuration program of the device of implementing an automatic password changing technology for cloud hosts and cloud bastion hosts, and the configuration program, when being executed by one or more processors, can implement the method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts in the present invention.

Compared with the conventional technology, the advantages of the present invention are as follows:

A method of implementing an automatic password changing technology for cloud hosts and cloud bastion hosts is developed in the present invention, through a connection between a cloud computing platform and an open-source cloud bastion hosts, automatic synchronization of cloud resources and cloud asset information in a cloud computing platform of cloud bastion hosts may be completed, and a password policy may be delivered by using the cloud computing platform, implementing automatic password changing for the cloud asset information in the cloud computing platform. According to the method, under universal management of the cloud platform, when random password changing for cloud asset information in all cloud computing platforms is completed, the information is synchronized with cloud bastion hosts, and after automatic password changing, a cloud tenant can directly log in to the cloud bastion hosts by using the cloud platform.

Through a seamless connection between a cloud computing platform and an open-source bastion host, cloud asset information in the cloud computing platform is synchronized in real time with cloud bastion hosts. The cloud computing platform uses cloud bastion hosts verification

module to ensure the accuracy of synchronizing the cloud asset information in the cloud computing platform. For a multi-cloud heterogeneous environment, only cloud asset information in one cloud computing platform needs to be maintained in the cloud computing platform, to ensure that an automatic password changing scheme can be normally performed.

Through a seamless connection between the cloud computing platform and the cloud bastion hosts, the linkage between the cloud computing platform and the cloud bastion hosts has solved the problem of isolation. An automatic password changing technology may be developed and released to cloud tenants as a cloud service of the cloud computing platform. The arrangement of an automatic password changing scheme for cloud resources can be completed by using only the cloud computing platform. The cloud bastion hosts may periodically perform batch password changing in a policy-based manner.

Through the connection between the cloud computing platform and the cloud bastion hosts, it may be satisfied that in service scenarios such as dynamic delivery and autoscaling of cloud resources, the timeliness of synchronization between the cloud asset information in the cloud computing platform and the information in the cloud bastion hosts is implemented. It is not necessary to manually maintain information in the cloud bastion hosts, so that manual costs are reduced. In addition, universal password management may be performed by using the cloud computing platform, to satisfy password changing policy requirements of different tenants, and improve the stability of automatic password changing.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows steps of a method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to the present invention.

FIG. 2 is a diagram of modules of a configuration program of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to the present invention.

FIG. 3 is a diagram of program modules of a password changing policy obtaining module in another configuration program of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to the present invention.

FIG. 4 is a specific flowchart of another method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts 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 embodiments of the

present invention with reference to the accompanying drawings in 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 other sequences than those illustrated or described. In addition, the terms "include", "comprise", and any variation of such terms in the description and claims of the present invention 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.

To make the advantages of the technical solutions of the present invention more comprehensible, the present invention is described below in detail with reference to the accompanying drawings and embodiments.

FIG. 1 shows steps of a method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to the present invention.

As shown in FIG. 1, the method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts provided in the present invention specifically includes the following steps:

Step S1: Deploy and fuse open-source cloud bastion hosts Jumpserver: construct cloud bastion hosts applicable to a cloud service scenario on a cloud computing platform by using their own open api interfaces of open-source cloud bastion hosts, implement a connection between the cloud computing platform and the cloud bastion hosts, and implement universal management and maintenance of cloud asset information in the cloud computing platform and cloud asset information in the cloud bastion hosts on the cloud computing platform; and simultaneously establish cloud bastion host verification module on the connected cloud computing platform, to verify and ensure , in a multi-cloud heterogeneous environment, accuracy of the cloud asset

information in the cloud computing platform synchronized between the cloud computing platform and the cloud bastion hosts, and ensure that an automatic password changing scheme can be normally performed.

In the present invention, the open-source cloud bastion hosts is not limited to the open-source cloud bastion hosts Jumpserver that is already used in this embodiment.

The cloud bastion hosts uses a distributed architecture, supports multi-room cross-area deployment, supports horizontal scaling, and has no amount and concurrency limitations on the cloud asset information in the cloud computing platform.

In this embodiment, cloud hosts includes various operating systems and versions (for example, Windows and Linux) of various cloud basic resource types (Vware, openstack, bare metal, and the like). Users are all cloud tenants in a cloud computing service platform. Application scenarios include service systems such as full-industry production, development, UAT, and test as well as universal scenarios. It needs to be noted that, during actual application, the solution provided in the present invention is not limited to users or application fields in the foregoing embodiment, and includes common devices, equipment, and the like understood in the field.

In step S1, the cloud bastion host verification module is used by the cloud computing platform to periodically and automatically complete a verification function and/or used by the cloud tenants to manually complete the verification function, to complete verification related to cloud asset information in the cloud hosts in the cloud computing platform by using an automation technology, verify correctness of the cloud asset information in an automatic remote login mode, simultaneously perform verification with the cloud bastion hosts, to ensure that the cloud asset information in the cloud platform is consistent with that in the cloud bastion, and when a verification result is that the information is consistent, initiate verification. The cloud asset information includes an ip of the cloud hosts, an operating system of the cloud hosts, a port, an account, and a password for remote login of the cloud hosts, and the like.

The cloud asset information in the cloud computing platform includes: basic information such as the ip and the port of the cloud hosts, operation permission information of a cloud tenant, and cloud resource account information of a plurality of accounts such as username and password information of an administrator user/a non-administrator user in resources of the cloud hosts. In this embodiment, one cloud asset corresponds to a plurality of pieces of cloud resource account information.

In this embodiment, the cloud bastion hosts is provided to the cloud tenants as one of services

provided by the cloud computing platform, and the cloud tenants can directly jump by using the cloud computing platform to use the cloud bastion hosts.

Step S2. Establish a fault tolerance mechanism response rule: establish a fault tolerance mechanism response rule added to the cloud computing platform, to enlarge a password difference among different systems, and to improve stability of automatic password changing, where the fault tolerance mechanism is an automatic password changing fault tolerance mechanism added when the cloud bastion host verification module is established on the cloud computing platform. The automatic password changing fault tolerance mechanism includes: during execution of an automatic password changing task, controlling to synchronously perform a password verification function one by one, after password changing is automatically completed, recording a previous password, and then recording a newly changed password together; next, attempting automatic verification on a new password of the cloud hosts, and if the verification fails, rolling back this task of the cloud hosts, to ensure that the old password can be used to log in; terminating all automatic password changing tasks, where manual intervention is required to choose to skip or continue; and if the verification succeeds, continuing to perform a next task.

Step S3. Establish a response rule for real-time synchronization of the cloud asset information in the cloud computing platform: establish a real-time response rule for the cloud asset information in the cloud computing platform in a service scenario such as dynamic delivery and autoscaling for the cloud asset information in the cloud computing platform, implementing real-time automatic synchronization related to the cloud asset information in the cloud computing platform and in the cloud bastion hosts on the cloud computing platform. The service scenario such as dynamic delivery and autoscaling includes: dynamic scaling of the resources of the cloud hosts, where a newly scaled cloud hosts has an independent account and password, and the independent account and password are synchronized with the cloud bastion hosts, to ensure operability of resources of the newly scaled cloud hosts.

Step S4: Obtain a password changing policy: obtain a scheduled task from the cloud computing platform for automatic password changing and self-defining, and determine a password changing policy according to the scheduled task, where the scheduled task obtained from the cloud computing platform for automatic password changing includes: a start time, a list of involved cloud hosts, users of the involved cloud hosts, and the like.

Step S5. Perform automatic password changing: after the automatic password changing policy is obtained, automatically invoke, in the cloud computing platform, the cloud computing platform and the cloud bastion hosts that are connected in step S1, to complete arrangement of the automatic

password changing policy for the cloud asset information in the cloud computing platform; automatically respond to the fault tolerance mechanism and the cloud bastion host verification module in step S2, and perform periodic automatic verification and perform batch password changing by using the cloud bastion hosts according to the automatic password changing policy; and synchronize a result of automatic execution from the cloud bastion hosts to the cloud computing platform by using step S3, where the result takes effect in a corresponding cloud hosts.

FIG. 2 is a diagram of modules of a configuration program of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to the present invention.

As shown in FIG. 2, a device of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts provided in the present invention includes:

an open-source cloud bastion host deployment and fusion module 101, configured to: construct cloud bastion hosts applicable to a cloud service scenario on a cloud computing platform by using open api interfaces of own open-source of cloud bastion hosts Jumpserver, implementing a connection between the cloud computing platform and the cloud bastion hosts, and implement universal management and maintenance of cloud asset information in the cloud computing platform and cloud asset information in the cloud bastion hosts on the cloud computing platform; and simultaneously establish cloud bastion host verification module on the connected cloud computing platform, to verify and ensure , in a multi-cloud heterogeneous environment, accuracy of the cloud asset information synchronized between the cloud computing platform and the cloud bastion hosts, and ensure that an automatic password changing scheme can be normally performed;

a fault tolerance mechanism response module 102, configured to: automatically respond to a fault tolerance mechanism rule, to enlarge a password difference among different systems, and to improve stability of automatic password changing, where the fault tolerance mechanism is an automatic password changing fault tolerance mechanism added when the cloud bastion host verification module is established on the cloud computing platform;

a response module 103 for real-time synchronization of cloud asset information in a cloud computing platform, configured to: automatically respond to a real-time synchronization rule for the cloud asset information in the cloud computing platform in a service scenario such as dynamic delivery and autoscaling for the cloud asset information in the cloud computing platform, implementing real-time automatic synchronization related to the cloud asset information in the

cloud computing platform and in the cloud bastion hosts on the cloud computing platform;

a password changing policy obtaining module 104, configured to: obtain a scheduled task from the cloud computing platform for automatic password changing and self-defining, and determine a password changing policy according to the scheduled task; and

an automatic password changing execution module 105, configured to: after the password changing policy is obtained, automatically invoke, in the cloud computing platform, the cloud computing platform and the cloud bastion hosts that are connected by the open-source cloud bastion hosts deployment and fusion module, to complete arrangement of the automatic password changing policy for the cloud asset information in the cloud computing platform; automatically respond to the fault tolerance mechanism and the cloud bastion host verification module in the fault tolerance mechanism response module, and perform periodic automatic verification and perform batch password changing by using the cloud bastion hosts according to the automatic password changing policy; and synchronize a result of automatic execution from the cloud bastion hosts to the cloud computing platform by using the response module for real-time synchronization of cloud asset information in a cloud computing platform, where the result takes effect in a corresponding cloud hosts.

In addition to the foregoing method of automatic password changing, the present invention further provides another method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts. The obtaining a password changing policy further includes customizing, by a cloud tenant, a password changing policy. FIG. 3 is a diagram of program modules of a password changing policy obtaining module in another device of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to the present invention.

FIG. 3 is a diagram of program modules of a password changing policy obtaining module in another device of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to the present invention. The password changing policy obtaining module 104 further includes:

a display submodule 1041, configured to display an interface of a module specially configured to perform an automatic password changing task of the cloud hosts in the cloud computing platform, so that a timing task of customizing automatic password changing that needs to be started can be provided to a user; and

a self-defining password changing policy submodule 1042, used for cloud tenants to directly

configure the cloud resource password changing plan through the cloud computing platform. After the configuration is completed, the self-defined automatic password changing policy is obtained.

In this embodiment, the cloud computing platform can be opened to any user with permission. Through the display submodule 1041, the interface of the module in the cloud computing platform dedicated to the automatic password changing task of the virtual machine is displayed on the user terminal interface, and the user can be provided user-defined scheduled tasks that need to enable automatic password change; And through a self-defining password changing policy submodule 1042, the cloud tenants can directly configure the cloud resource password changing plan through the cloud computing platform, and get the self-defined automatic password changing policy after configuration.

In this embodiment, the implementation process of automatic password change is further described.

FIG. 4 is a specific flowchart of another method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to the present invention.

As shown in FIG. 4, automation of a cloud service of automatic password changing is established by using the open-source cloud bastion hosts deployment and fusion module 101, the fault tolerance mechanism response module 102, the response module 103 for real-time synchronization of cloud asset information in a cloud computing platform, the password changing policy obtaining module 104, and the automatic password changing execution module 105. By taking advantage of the automation capability of cloud services, the cloud resource account information of cloud tenants can be synchronized in the cloud computing platform, and the cloud tenants can achieve the fault-tolerant judgment mechanism of remote control, login verification, password change, N-time verification, etc. through the cloud computing platform, to achieve the fault-tolerant capability of automatic password change of cloud fortress machines and achieve automatic password change.

The cloud computing platform automatically obtains, by using the automatic password changing policy obtaining module 104, a scheduled task obtained from the cloud computing platform for automatic password changing, determines a password changing policy according to the scheduled task, automatically performs password changing for the cloud hosts by using the automatic password changing execution module 105, and performs remote login verification based on asset information of the cloud computing platform and the cloud bastion hosts, to enter the cloud

bastion host verification module.

In this embodiment, the self-defined password changing scheme further includes an automatic password changing policy self-defined by the cloud tenants. During the self-defining of the cloud tenants, the self-defining of the automatic password changing policy is implemented by editing a password changing scheme, and includes: configuring basic settings of a display interface, including: configuring basic content such as name, remarks, an account type, a password changing execution time; and setting resources on the display interface, where a visual click window component and a search window component are set on the interface, and candidate items are set, which are primary common basic settings in an existing password changing configuration and are used for direct selection by the cloud tenants without performing a search. If a user has a specific requirement or makes a query, the user may directly perform a keyword search in a search window and then perform a click for confirmation. If a user has a specific requirement or search, the user may directly perform a keyword search in a search window and then click to confirm. The self-defined scheme may include basic maintenance, change, and debugging, including sharing, recreation, and the like.

The cloud bastion host verification module completes verification related to cloud asset information in the cloud hosts by using an automation technology, where the information includes an ip of the cloud hosts, an operating system of the cloud hosts, a port, an account, and a password for remote login of the cloud hosts, and the like, and verifies correctness of the cloud asset information in an automatic remote login mode, simultaneously performs verification with the cloud bastion hosts, to ensure that the cloud asset information in the cloud platform is consistent with that in the cloud bastion. When a verification result is that the information is consistent, the verification succeeds, and verification is initiated to enter an automatic password changing phase. N times of verification is performed after [password changing success 1] is triggered. Password changing succeeds when the verification succeeds, where the result takes effect in the cloud hosts. In addition, the cloud asset information is updated and cloud bastion hosts asset information is simultaneously synchronized. The cloud bastion hosts is provided to the cloud tenants as one of services provided by the cloud computing platform. the cloud tenants may directly jump or perform a single-point login by using the cloud computing platform to use the cloud bastion hosts.

If the verification fails or automatic password changing fails in the cloud bastion host verification module, the fault tolerance module is entered to automatically respond to the fault tolerance mechanism and return to the cloud computing platform. A specific process includes: during execution of an automatic password changing task, controlling to perform a password

verification function one by one at the backend in parallel in batches, after password changing is automatically completed, recording a previous password, and then recording a newly changed password together; next, attempting automatic verification on a new password of the cloud hosts, and if the verification fails, rolling back this task of the cloud hosts, to ensure that the old password can be used to log in; terminating all automatic password changing tasks, where manual intervention is required to choose to skip or continue; and if the verification succeeds, continuing to perform the next task.

The present invention further includes an electronic device. The device includes a memory and a processor. The memory stores a configuration program that can run, on the processor, the device provided in this embodiment. The configuration program, when being executed by the processor, can implement the method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts provided in this embodiment.

The present invention further includes a computer-readable storage medium. The computer-readable storage medium stores a configuration program of the device provided in this embodiment. The configuration program, when being executed by one or more processors, can implement the method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts provided 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 of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts, wherein the method specifically comprises the following steps:

S1. deploying and fusing open-source cloud bastion hosts: constructing cloud bastion hosts applicable to a cloud service scenario on a cloud computing platform by using their own open api interfaces of open-source cloud bastion hosts, implement a connection between the cloud computing platform and the cloud bastion hosts, and implement universal management and maintenance of cloud asset information in the cloud computing platform and cloud asset information in the cloud bastion hosts on the cloud computing platform; and simultaneously establishing cloud bastion host verification module on the connected cloud computing platform, to verify and ensure , in a multi-cloud heterogeneous environment, accuracy of the cloud asset information in the cloud computing platform synchronized between the cloud computing platform and the cloud bastion hosts, and ensure that an automatic password changing scheme can be normally performed;

S2. establishing a fault tolerance mechanism response rule: establishing a fault tolerance mechanism response rule added to the cloud computing platform, to enlarge a password difference among different systems, and to improve stability of automatic password changing, wherein the fault tolerance mechanism is an automatic password changing fault tolerance mechanism added when the cloud bastion host verification module is established on the cloud computing platform;

S3. establishing a response rule for real-time synchronization of the cloud asset information in the cloud computing platform: in a cloud computing platform service scenario such as the cloud asset information dynamic delivery and the cloud asset information autoscaling,etc, establishing a real-time response rule for the cloud asset information in the cloud computing platform, on the cloud computing platform, implementing real-time automatic synchronization related to the cloud asset information in the cloud computing platform and in the cloud bastion hosts ;

S4. obtaining a password changing policy: obtaining a scheduled task from the cloud computing platform for automatic password changing and self-defining, and determining a password changing policy according to the scheduled task; and

S5. performing the automatic password changing: after the automatic password

CLAIMS

changing policy is obtained, automatically invoking, in the cloud computing platform, the cloud computing platform and the cloud bastion hosts that are connected in step S1, to complete arrangement of the automatic password changing policy for the cloud asset information in the cloud computing platform; automatically responding to the fault tolerance mechanism and the cloud bastion host verification module in step S2, and performing periodic automatic verification and performing batch password changing by using the cloud bastion hosts according to the automatic password changing policy; and synchronizing a result of automatic execution from the cloud bastion hosts to the cloud computing platform by performing step S3, wherein the result takes effect in the corresponding cloud hosts.

2. The method of an automatic password changing technology according to claim 1, wherein

in step S1, the cloud bastion hosts uses a distributed architecture, supports multi-room cross-area deployment, supports horizontal scaling, and has no amount and concurrency limitations of the cloud asset information in the cloud computing platform;

the cloud asset information in the cloud computing platform comprises: basic information such as an ip and a port of the cloud hosts, operation permission information of a cloud tenant, and cloud resource account information of a plurality of accounts such as username and password information of an administrator user/a non-administrator user in resources of the cloud hosts; and

the cloud bastion hosts is provided to the cloud tenants as one of services provided by the cloud computing platform, and the cloud tenants can directly jump by using the cloud computing platform to use the cloud bastion hosts.

3. The method of an automatic password changing technology according to claim 1 or 2, wherein

in step S1, the cloud bastion host verification module is used by the cloud computing platform to periodically and automatically complete a verification function and/or used by the cloud tenants to manually complete the verification function, using an automation technology in the cloud computing platform to complete verification of relevant cloud asset information in the cloud hosts, and verifying correctness of the cloud asset information in an automatic remote login mode, simultaneously performing verification with the cloud bastion hosts, to ensure that the cloud asset information in the cloud platform is

CLAIMS

consistent with the cloud asset information in the cloud bastion, and when the information of the verification result is consistent, initiating verification of relevant cloud asset information.

4. The method of an automatic password changing technology according to any one of claims 1 to 3, wherein

in step S2, the automatic password changing fault tolerance mechanism comprises: during execution of an automatic password changing task, controlling to synchronously perform a password verification function one by one, after the password changing is automatically completed, recording a previous password, and then recording a newly changed password together; next, attempting automatic verification on a new password of the cloud hosts, and if the verification fails, rolling back this task of the cloud hosts, to ensure that the old password can be used to log in; terminating all automatic password changing tasks, wherein manual intervention is required to choose to skip or continue; and if the verification succeeds, continuing to perform a next task.

5. The method of an automatic password changing technology according to claim 1, wherein

in step S3, the service scenario such as dynamic delivery and autoscaling comprises: a dynamic scaling of the resources of the cloud hosts, wherein a newly scaled cloud hosts has an independent account and an independent password which are synchronized with the cloud bastion hosts, to ensure operability of resources of the newly scaled cloud hosts.

6. The method of an automatic password changing technology according to claim 1, wherein

in step S4, the scheduled task obtained from the cloud computing platform for the automatic password changing and self-defining comprises: a start time, a list of the involved cloud hosts, users of the involved cloud hosts, and the like.

7. A device of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts, wherein the device comprises:

an open-source cloud bastion host deployment and fusion module, configured to: construct cloud bastion hosts applicable to a cloud service scenario on a cloud computing platform by using their own open api interfaces of open-source cloud bastion hosts, implement a connection between the cloud computing platform and the cloud bastion hosts, and implement universal management and maintenance of cloud asset information in the

CLAIMS

cloud computing platform and cloud asset information in the cloud bastion hosts on the cloud computing platform; and simultaneously establish cloud bastion host verification module on the connected cloud computing platform, to verify and ensure , in a multi-cloud heterogeneous environment, accuracy of the cloud asset information in the cloud computing platform synchronized between the cloud computing platform and the cloud bastion hosts, and ensure that an automatic password changing scheme can be normally performed;

a fault tolerance mechanism response module, configured to: automatically respond to a fault tolerance mechanism rule, to enlarge a password difference among different systems, and to improve stability of automatic password changing, wherein the fault tolerance mechanism is an automatic password changing fault tolerance mechanism added when the cloud bastion host verification module is established on the cloud computing platform;

a response module for real-time synchronization of cloud asset information in a cloud computing platform, configured to: in a cloud computing platform service scenario such as the cloud asset information dynamic delivery and the cloud asset information autoscaling,etc, automatically respond a real-time synchronization rule for the cloud asset information in the cloud computing platform, and implement real-time automatic synchronization related to the cloud asset information in the cloud computing platform and in the cloud bastion hosts on the cloud computing platform;

a password changing policy obtaining module, configured to: obtain a scheduled task from the cloud computing platform for automatic password changing and self-defining, and determine a password changing policy according to the scheduled task; and

an automatic password changing execution module, configured to: after the automatic password changing policy is obtained, automatically invoke, in the cloud computing platform, the cloud computing platform and the cloud bastion hosts that are connected by the open-source cloud bastion hosts deployment and fusion module, to complete arrangement of the automatic password changing policy for the cloud asset information in the cloud computing platform; automatically respond to the fault tolerance mechanism and the cloud bastion host verification module in the fault tolerance mechanism response module, and perform periodic automatic verification and perform batch password changing by using the cloud bastion hosts according to the automatic password changing policy; and synchronize a result of automatic execution from the cloud bastion hosts to the cloud computing platform by using the response module for real-time synchronization of cloud

CLAIMS

asset information in a cloud computing platform, wherein the result takes effect in a corresponding cloud hosts.

8. The device of an automatic password changing technology according to claim 7, wherein

the password changing policy obtaining module further comprises:

a display submodule, configured to display an interface of a module specially configured to perform an automatic password changing task of the cloud hosts in the cloud computing platform, so that a timing task of customizing automatic password changing that needs to be started can be provided to a user; and

A self-defining password changing policy submodule, configured to enable a cloud tenant to directly configure a cloud resource password changing scheme by using the cloud computing platform, to obtain a self-defined automatic password changing policy after the configuration is completed.

9. An electronic device, wherein the device comprises a memory and a processor, the memory stores a configuration program that can run the device according to claim 7 or 8 on the processor, and the configuration program, when being executed by the processor, can implement the method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to any one of claims 1 to 6.

10. A computer-readable storage medium, wherein the computer-readable storage medium stores a configuration program of the device according to claim 7 or 8, and the configuration program, when being executed by one or more processors, can implement the method of implementing automatic password changing with a fault tolerance mechanism for cloud hosts and cloud bastion hosts according to any one of claims 1 to 6.