

面向云主机和云堡垒机实现含容错机制的自动改密的方法

技术领域

本发明涉及云计算以及信息安全技术领域，具体涉及一种面向云主机和云堡垒机实现含容错机制的自动改密的方法。

背景技术

云主机是云计算在基础设施应用上的重要组成部分，位于云计算产业链金字塔底层，产品源自云计算平台。该平台整合了互联网应用三大核心要素：计算、存储、网络，面向用户提供公用化的互联网基础设施服务。云主机是一种类似 VPS 主机的虚拟化技术，VPS 是采用虚拟软件，VZ 或 VM 在一台主机上虚拟出多个类似独立主机的部分，能够实现单机多用户，每个部分都可以做单独的操作系统，管理方法同主机一样。而随着云主机云计算的发展的网络安全问题也不容忽视。

堡垒机作为云计算平台安全体系重要部件，堡垒机承担着在混合云环境下进行安全合规审计的关键作用，同时也面临许多问题：基础设施高度异构化、分布范围广；混合云中的云资源规模持续增长，需要堡垒机具备充分的可扩展性；云动态资源交付和弹性伸缩情况下的云资源管理及自动改密。

由于企业内部的传统物理设备、虚拟化平台、私有云，以及公有云，导致云计算平台的建设引入了大量不同类型的 IT 基础设施，而为了降低平台资源管理的难度，很好的适配云计算平台的 API 接口，又要求堡垒机能够在资产接入和管理上有较好的适配性和灵活性；另外，由于目前云计算平台拥有多企业、多组织、多租户，导致 IT 资产分布范围广，管理也相对分散。基于堡垒机构建的运维安全审计系统需要提供多级授权管理体系，以适配当前的 IT 管理模式

基础设施高度异构化、分布范围广，密码等信息维护人工成本高。云计算平台的建设引入了大量不同类型的 IT 基础设施，包括企业内部的传统物理裸金属设备、云计算虚拟化资源等。传统堡垒机在资产接入和管理上未有较好的适配性和灵活性，而传统模式下，云主机的账户新增、删除、修改等都需要人工在云资源和堡垒机两边先后完成配置，人工维护成本高，准确性和实时性都不够。

云计算平台与传统堡垒机的孤立性，难以实现实时联动自动改密。云计算平台与传统堡垒机相对孤立，云计算平台租户与堡垒机用户难以联动，往往需要手工同步维护云计算平台资源与堡垒机资源，由于传统堡垒机和云计算平台的孤立性，云计算平台难以通过云计算平台策略化的进行定期自动改密。

云动态资源交付和弹性伸缩情况下的云资源管理难度大，自动改密不稳定。由于云资源的动态交付和弹性伸缩的灵活性，资源的变化以及信息维护往往需要人工手动进行维护，时效性很差，往往会遇到堡垒机因信息维护不及时和信息维护错误等问题导致使用异常，自动改密存在不稳定因素。

因此，如何解决云计算平台的基础设施高度异构化、分布散乱、云计算平台与传统堡垒机的孤立性导致的难以实现自动改密及即便实现了也存在自动改密不稳定等问题，是目前亟待解决的技术问题。

发明内容

为解决云计算平台的基础设施高度异构化、分布散乱、云计算平台与传统堡垒机的孤立性导致的难以实现自动改密及实现后的自动改密不稳定等问题，本发明开发了一种面向云主机和云堡垒机实现含容错机制的自动改密的方法，可完成云计算平台与堡垒机的云计算平台中云资产信息自动同步，可通过云计算平台下发密码策略，实现云计算平台中云资产信息自动改密；实现了在云平台的统一管理下，完成对所有云计算平台中云资产信息随机改密的同时将这些信息与云堡垒机的同步，并实现在自动改密后，云租户直接通过云平台，登入云堡垒机。

本发明请求保护以下技术方案：

云计算平台通过与开源堡垒机的api接口的对接和功能开发，完成了云计算平台和云堡垒机的关于云计算平台中云资产信息的自动同步，实现云计算平台与堡垒机的无缝衔接，不再需要人工进行两套系统信息维护，云计算平台中云资产信息只需在云计算平台上维护即可。

云计算平台通过自主研发的堡垒机校验模块，利用云计算服务编排技术，研发了云资源自动改密技术，可直接在云计算平台设置云计算平台中云资产信息改密计划，通过云计算平台与开源堡垒机的对接，完成自动改密与信息同步。

云计算平台加入自动改密容错机制，提升自动改密稳定性，支持策略化的定期批量改密，增加不同系统之间密码差异化，提升复杂度以满足管理需求，以满足不同业务场景对云资源安全合规性的需求。

具体的：

本发明提供一种面向云主机和云堡垒机实现含容错机制的自动改密的方法，其特征在于，具体包括以下步骤：

S1 部署并融合开源堡垒机，通过开源堡垒机自身的开放的 api 接口在云计算

平台上构建了适合云业务场景的云堡垒机，实现云计算平台与云堡垒机的对接，及实现所述云计算平台的云资产信息与所述云堡垒机的云资产信息在云计算平台上进行统一管理和维护；同时在对接后的云计算平台上建立云堡垒机校验模块，用于确保在多云异构环境下，以验证和确保云计算平台与云堡垒机之间同步的所述云计算平台中云资产信息的准确性，保证自动改密计划能正常执行；

S2 建立容错机制响应规则，建立在云计算平台中加入的容错机制响应规则，用于增加不同系统之间密码差异化，提升自动改密稳定性；其中，所述容错机制是指在云计算平台建立云堡垒机校验模块时，加入的自动改密容错机制；

S3 建立实时同步云计算平台中云资产信息的响应规则，建立在云计算平台中云资产信息动态交付和弹性伸缩等业务场景下的云计算平台中云资产信息的实时响应规则，实现所述云堡垒机和云计算平台的关于云计算平台中云资产信息实时自动同步；

S4 获取改密策略，获取云计算平台对自动改密自定义的计划任务，根据所述计划任务确定改密策略；

S5 执行自动改密，在获取自动改密策略后，云计算平台中自动调用步骤 S1 所对接的云计算平台与云堡垒机，完成所述云计算平台中云资产信息的自动改密策略的编排；自动响应步骤 S2 中的容错机制及所述云堡垒机校验模块并通过所述云堡垒机按照所述自动改密策略进行的定期自动校验及执行批量改密；并通过步骤 S3 将自动执行的结果由所述云堡垒机同步至所述云计算平台，并在对应的所述云主机中生效。

进一步的，在所述步骤 S1 中，所述云堡垒机采用分布式架构，支持多机房跨区域部署，支持横向扩展，无云计算平台中云资产信息数量及并发限制；

所述云计算平台中云资产信息包含：云主机的 ip 及端口等基础信息、云租户的操作权限信息、云主机资源中管理员用户/非管理员用户的用户名和密码信息等多个账户的云资源账户信息；

所述云堡垒机作为云计算平台提供的服务之一提供给云租户，云租户通过云计算平台可直接跳转使用云堡垒机。

进一步的，在所述步骤 S1 中，所述云堡垒机校验模块是，用于云计算平台定期自动或/和云租户手动完成校验功能，在云计算平台中通过自动化技术完成对相关云主机云资产信息校验，通过自动远程登入的方式验证其正确性，同时再与云堡垒机进行校验，保证云平台中云资产信息与云堡垒机中一致，当验证结果一

致时，发起验证。

进一步的，在所述步骤 S2 中，所述自动改密容错机制包括：控制在自动改密任务执行的时候，同步逐条进行密码校验功能，在自动完成密码修改后，会记录之前的密码，再将新修改的密码一并记录；然后进行尝试自动的云主机新密码校验，若校验失败，则此条云主机任务回退，确保老密码可以登入；所有自动改密任务终止，需要人工介入，选择跳过或继续；若校验正确，则继续下一条任务。

进一步的，在所述步骤 S3 中，所述动态交付和弹性伸缩等业务场景包括：通过云主机资源的动态伸缩，新伸展出来的云主机将具有独立的账号和密码，所述独立的账号和密码将与所述云堡垒机进行同步，以保证新生云主机资源的可操作性。

进一步的，在所述步骤 S4 中，所述云计算平台对自动改密自定义的计划任务，包含：开始时间、涉及云主机清单、涉及云主机的使用者等。

本发明还提供一种面向云主机和云堡垒机实现含容错机制的自动改密的装置，其特征在于，包括：

部署并融合开源堡垒机模块，用于通过开源堡垒机自身的开放的 api 接口在云计算平台上构建了适合云业务场景的云堡垒机，实现云计算平台与云堡垒机的对接，及实现所述云计算平台的云资产信息与所述云堡垒机的云资产信息在云计算平台上进行统一管理和维护；同时在对接后的云计算平台上建立云堡垒机校验模块，用于确保在多云异构环境下，以验证和确保云计算平台与云堡垒机之间同步的所述云计算平台中云资产信息的准确性，保证自动改密计划能正常执行；

容错机制响应模块，用于自动响应容错机制的规则，用于增加不同系统之间密码差异化，提升自动改密稳定性；其中，所述容错机制是在云计算平台建立云堡垒机校验模块时，加入的自动改密容错机制；

实时同步云计算平台中云资产信息响应模块，用于自动响应在云计算平台中云资产信息动态交付和弹性伸缩等业务场景下的云计算平台中云资产信息的实时同步的规则，实现所述云堡垒机和云计算平台的关于云计算平台中云资产信息实时自动同步；

获取改密策略模块，用于获取云计算平台对自动改密自定义的计划任务，根据所述计划任务确定改密策略；

执行自动改密模块，用于在获取自动改密策略后，云计算平台中自动调用所述部署并融合开源堡垒机模块对接的云计算平台与云堡垒机，完成所述云计算平

台中云资产信息的自动改密策略的编排；自动所述容错机制响应模块中的容错机制及所述云堡垒机校验模块并通过所述云堡垒机按照所述自动改密策略进行的定期自动校验及执行批量改密；并通过所述实时同步云计算平台中云资产信息响应模块，将自动执行的结果由所述云堡垒机同步至所述云计算平台，并在对应的所述云主机中生效。

进一步的，所述获取改密策略模块还包括：

显示子模块，用于显示云计算平台中专门用于云主机自动改密任务的模块的界面，可以提供用户自定义所需要启用自动改密的定时任务；

自定义改密策略子模块，云租户通过云计算平台可直接配置云资源改密计划，配置完成后得到自定义的自动改密策略。

本发明还包括一种电子装置，其特征在于，该装置包括存储器、处理器，所述存储器上存储有可在所述处理器上运行本发明所述的一种面向云主机和云堡垒机实现自动改密技术的装置的配置程序，所述配置程序被所述处理器执行时可以实现本发明所述的一种面向云主机和云堡垒机实现含容错机制的自动改密的方法。

本发明还包括一种计算机可读存储介质，其特征在于，所述计算机可读的存储介质上存储有本发明所述的一种面向云主机和云堡垒机实现自动改密技术的装置的配置程序，所述配置程序可以被一个或多个处理器执行，以实现本发明所述的一种面向云主机和云堡垒机实现含容错机制的自动改密的方法。

与现有技术相比，本发明的优点在于：

本发明开发了一种面向云主机和云堡垒机实现自动改密技术的方法，通过云计算平台与开源堡垒机的对接，可完成云资源与堡垒机的云计算平台中云资产信息自动同步，可通过云计算平台下发密码策略，实现云计算平台中云资产信息自动改密；解决了在云平台的统一管理下，完成对所有云计算平台中云资产信息随机改密的同时将这些信息与云堡垒机的同步，并实现在自动改密后，云租户直接通过云平台，登入云堡垒机。

通过云计算平台与开源堡垒无缝的对接，云计算平台中云资产信息将与云堡垒机实时同步，云计算平台通过云堡垒机校验模板以确保云计算平台中云资产信息同步的准确性，针对多云异构环境，也只需在云计算平台维护一套云计算平台中云资产信息，保证自动改密计划能正常执行。

通过云计算平台整与云堡垒无缝的对接，云计算平台与云堡垒机之间的联动使孤立性问题得以解决，自动改密技术可以作为云计算平台的一项云服务进行发布开发给各云租户，只需通过云计算平台即可完成云资源自动改密计划的编排，云堡垒机可策略化的定期执行批量改密。

通过云计算平台与云堡垒机的对接，可满足云资源动态交付和弹性伸缩等业务场景下实现云计算平台中云资产信息与云堡垒机信息同步时效性，无需手工进行堡垒机信息维护，降低了人工成本。同时可通过云计算平台进行密码统一管理，满足不同租户改密策略需求，提升自动改密的稳定性。

附图说明

图 1. 本发明提供的一种面向云主机和云堡垒机实现含容错机制的自动改密的方法步骤。

图 2. 本发明提供的一种面向云主机和云堡垒机实现含容错机制的自动改密的配置程序模块图。

图 3. 本发明提供的另外一种面向云主机和云堡垒机实现含容错机制的自动改密配置程序中的获取改密策略模块的程序模块图。

图 4. 是本发明提供的另外一种面向云主机和云堡垒机实现含容错机制的自动改密的方法的具体流程图。

具体实施方式

为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于涵盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统，产品或设备不必限于清楚地列出的那些步骤或单

元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

为使本发明技术方案的优点更加清楚，下面结合附图和实施例对本发明做详细说明。

图 1 是本发明提供的一种面向云主机和云堡垒机实现含容错机制的自动改密的方法步骤。

如图 1 所示，本发明提供的一种面向云主机和云堡垒机实现含容错机制的自动改密的方法，其中，具体包括以下步骤：

步骤 S1 部署并融合 Jumpserver 开源堡垒机，通过开源堡垒机自身的开放的 api 接口在云计算平台上构建了适合云业务场景的云堡垒机，实现云计算平台与云堡垒机的对接，及实现所述云计算平台的云资产信息与所述云堡垒机的云资产信息在云计算平台上进行统一管理和维护；同时在对接后的云计算平台上建立云堡垒机校验模块，用于确保在多云异构环境下，以验证和确保云计算平台与云堡垒机之间的同步的所述云计算平台中云资产信息的准确性，保证自动改密计划能正常执行。

在本发明中，所述的开源堡垒机不限于本实施例已经利用的 Jumpserver 开源堡垒机。

所述云堡垒机采用分布式架构，支持多机房跨区域部署，支持横向扩展，无云计算平台中云资产信息数量及并发限制。

本实施例中涉及的云主机包含各种云基础资源种类的（Vware、openstack、裸金属等）上的各种操作系统及版本（如：windows、linux），涉及的用户是云计算服务平台中所有的云租户，应用场景：全行业的生产、开发、UAT、测试等业务系统，通用型。需要注意的是，实际应用中，本发明提供的方案不仅限于上述实施例所述用户或应用领域，包括本领域理解的常用的装置设备等。

在所述步骤 S1 中，所述云堡垒机校验模块是，用于云计算平台定期自动或/和云租户手动完成校验功能，在云计算平台中通过自动化技术完成对相关云主机云资产信息校验，通过自动远程登入的方式验证其正确性，同时再与云堡垒机进行校验，保证云平台中云资产信息与云堡垒机中一致，当验证结果一致时，发起验证。其中云资产信息包括云主机 ip、云主机操作系统、云主机远程登入的端口、账户、密码等。

所述云计算平台中云资产信息包含：云主机的 ip 及端口等基础信息、云租

户的操作权限信息、云主机资源中管理员用户/非管理员用户的用户名和密码信息等多个账户的云资源账户信息。在本实施例中，一个云资产对应多个云资源账户信息。

在本实施例中，所述云堡垒机作为云计算平台提供的服务之一提供给云租户，云租户通过云计算平台可直接跳转使用云堡垒机。

步骤 S2 建立容错机制响应规则，建立在云计算平台中加入的容错机制响应规则，用于增加不同系统之间密码差异化，提升自动改密稳定性；其中，所述容错机制是在云计算平台建立云堡垒机校验模块时，加入的自动改密容错机制；所述自动改密容错机制包括：控制在自动改密任务执行的时候，同步逐条进行密码校验功能，在自动完成密码修改后，会记录之前的密码，再将新修改的密码一并记录；然后进行尝试自动的云主机新密码校验，若校验失败，则此条云主机任务回退，确保老密码可以登入；所有自动改密任务终止，需要人工介入，选择跳过或继续；若校验正确，则继续下一条任务。

步骤 S3 建立实时同步云计算平台中云资产信息的响应规则，建立在云计算平台中云资产信息动态交付和弹性伸缩等业务场景下的云计算平台中云资产信息的实时响应规则，实现所述云堡垒机和云计算平台的关于云计算平台中云资产信息实时自动同步；所述动态交付和弹性伸缩等业务场景包括：通过云主机资源的动态伸缩，新伸展出来的云主机将具有独立的账号和密码，所述独立的账号和密码将与所述云堡垒机进行同步，以保证新生云主机资源的可操作性。

步骤 S4 获取改密策略，获取云计算平台对自动改密自定义的计划任务，根据所述计划任务确定改密策略；所述云计算平台对自动改密自定义的计划任务，包含：开始时间、涉及云主机清单、涉及云主机的使用者等。

步骤 S5 执行自动改密，在获取自动改密策略后，云计算平台中自动调用步骤 S1 所对接的云计算平台与云堡垒机，完成所述云计算平台中云资产信息的自动改密策略的编排；自动响应步骤 S2 中的容错机制及所述云堡垒机校验模块并通过所述云堡垒机按照所述自动改密策略进行的定期自动校验及执行批量改密；并通过步骤 S3 将自动执行的结果由所述云堡垒机同步至所述云计算平台，并在对应的所述云主机中生效。

图 2 是本发明提供的一种面向云主机和云堡垒机实现含容错机制的自动改密的配置程序模块图。

如图2所示，本发明提供一种面向云主机和云堡垒机实现含容错机制的自动

改密的装置，其中，包括：

部署并融合开源堡垒机模块 101，用于通过 Jumpserver 开源堡垒机自身的开放的 api 接口在云计算平台上构建了适合云业务场景的云堡垒机，实现云计算平台与云堡垒机的对接，及实现所述云计算平台的云资产信息与所述云堡垒机的云资产信息在云计算平台上进行统一管理和维护；同时在对接后的云计算平台上建立云堡垒机校验模块，用于确保在多云异构环境下，以验证和确保云计算平台与云堡垒机之间的同步的所述云资产信息的准确性，保证自动改密计划能正常执行；

容错机制响应模块 102，用于自动响应容错机制的规则，用于增加不同系统之间密码差异化，提升自动改密稳定性；其中，所述容错机制是在云计算平台建立云堡垒机校验模块时，加入的自动改密容错机制；

实时同步云计算平台中云资产信息响应模块 103，用于自动响应在云计算平台中云资产信息动态交付和弹性伸缩等业务场景下的云计算平台中云资产信息的实时同步的规则，实现所述云堡垒机和云计算平台的关于云计算平台中云资产信息实时自动同步；

获取改密策略模块 104，用于获取云计算平台对自动改密自定义的计划任务，根据所述计划任务确定改密策略；

执行自动改密模块 105，用于在获取自动改密策略后，云计算平台中自动调用所述部署并融合开源堡垒机模块对接的云计算平台与云堡垒机，完成所述云计算平台中云资产信息的自动改密策略的编排；自动所述容错机制响应模块中的容错机制及所述云堡垒机校验模块并通过所述云堡垒机按照所述自动改密策略进行的定期自动校验及执行批量改密；并通过所述实时同步云计算平台中云资产信息响应模块，将自动执行的结果由所述云堡垒机同步至所述云计算平台，并在对应的所述云主机中生效。

除上述自动改密的方法之外，本发明还提供另外一种面向云主机和云堡垒机实现含容错机制的自动改密的方法，其中，所述获取改密策略其中还包括云租户自定义改密策略。图 3 是本发明提供的另一种面向云主机和云堡垒机实现含容错机制的自动改密装置中的获取改密策略模块的程序模块图。

在图 3 中，本发明提供了另外一种面向云主机和云堡垒机实现含容错机制的自动改密装置中的获取改密策略模块的程序模块图。其中，获取改密策略模块 104 还包括：

显示子模块 1041，用于显示云计算平台中专门用于云主机自动改密任务的

模块的界面，可以提供用户自定义所需要启用自动改密的定时任务；

自定义改密策略子模块 1042，用于云租户通过云计算平台可直接配置云资源改密计划，配置完成后得到自定义的自动改密策略。

在本实施例中，云计算平台通过云平台自身的权限管控可以开放给任何有权限的用户。通过显示子模块 1041，在用户终端界面上显示出云计算平台中专门用于云主机自动改密任务的模块的界面，可以提供用户自定义所需要启用自动改密的定时任务；并通过自定义改密策略子模块 1042，使得云租户自己可以通过云计算平台可直接配置云资源改密计划，配置完成后得到自定义的自动改密策略。

本实施例中通过对自动改密的实现流程进一步进行说明。

图 4 是本发明提供的另外一种面向云主机和云堡垒机实现容错机制的自动改密的方法的具体流程图。

如图 4 所示，通过上述部署并融合开源堡垒机模块 101、容错机制响应模块 102、实时同步云计算平台中云资产信息响应模块 103、获取改密策略模块 104、执行自动改密模块 105，建立了自动改密的云服务自动化；通过利用云服务的自动化的能力，可以使得云租户的云资源账户信息在云计算平台中实现同步、使得云租户可以通过云计算平台远程控制、登录校验、改密、N 次校验等的容错判断机制，实现云堡垒机自动改密的容错能力并实现自动改密。

云计算平台自动的通过获取改密策略模块 104，获取云计算平台对自动改密自定义的计划任务，根据所述计划任务确定改密策略，通过执行自动改密模块 105 自动进行云主机改密；根据云计算平台与堡垒机的资产信息运行远程登入校验，进入云堡垒机校验模块。

其中，在本实施例中，所述的自定义改密计划还包括云租户自定义配置的自动改密策略：在云租户自定义配置过程中，通过编辑改密计划实现自定义的自动改密策略的配置，包括：在显示界面对基础设置进项配置，包括对基本内容，如名称、备注、账户类型、改密执行时间的配置。还包括在显示界面对资源进行的设置，界面设置有可视化点选窗口组件以及搜索窗口组件，并设置有候选项，是现有改密配置中主要常用的基础设置，用于云租户直接选择无需进行搜索；如果用户有特定需求或查询，可以在搜索窗口直接进行关键字搜索后再进行点选确认。自定义配置好的计划可以进行基本的维护和修改调试，包括分享、再创建等。

云堡垒机校验模块通过自动化技术完成对相关云主机云资产信息校验，包括云主机 ip、云主机操作系统、云主机远程登入的端口、账户、密码等，通过自动

远程登入的方式验证其正确性，同时再与云堡垒机进行校验，保证云平台中云资产信息与云堡垒中一致，当校验结果一致时，校验成功，发起验证进入自动改密阶段。在触发[改密成功 1]后进入 N 次校验，验证成功则改密成功，在云主机中自动生效，同时更新云资产信息并同时同步云堡垒机资产信息，云堡垒机作为云计算平台提供的服务之一提供给云租户，云租户可以通过云计算平台可直接跳转或单点登入使用云堡垒机。

如果在云堡垒机校验模块中校验失败或自动改密失败，进入容错模块，则自动响应容错机制，返回至云计算平台；具体过程包括：控制在自动改密任务执行的时候，后台并行分批次逐条进行密码校验功能，在自动完成密码修改后，会记录之前的密码，再将新修改的密码一并记录；然后进行尝试自动的云主机新密码校验，若校验失败，则此条云主机任务回退，确保老密码可以登入；所有自动改密任务终止，需要人工介入，选择跳过或继续；若校验正确，则继续下一条任务。

在本发明中还包括一种电子装置，其中，该装置包括存储器、处理器，所述存储器上存储有可在所述处理器上运行如本实施例提供的装置的配置程序，所述配置程序被所述处理器执行时可以实现如本实施例提供的一种面向云主机和云堡垒机实现含容错机制的自动改密的方法。

在本发明中还包括一种计算机可读存储介质，其特征在于，所述计算机可读的存储介质上存储有如本实施例提供的装置的配置程序，所述配置程序可以被一个或多个处理器执行，以实现如本实施例提供的一种面向云主机和云堡垒机实现含容错机制的自动改密的方法。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

权利要求书

1、面向云主机和云堡垒机实现含容错机制的自动改密的方法，其特征在于，具体包括以下步骤：

S1 部署并融合开源堡垒机，通过开源堡垒机自身的开放的 api 接口在云计算平台上构建了适合云业务场景的云堡垒机，实现云计算平台与云堡垒机的对接，及实现所述云计算平台的云资产信息与所述云堡垒机的云资产信息在云计算平台上进行统一管理和维护；同时在对接后的云计算平台上建立云堡垒机校验模块，用于确保在多云异构环境下，以验证和确保云计算平台与云堡垒机之间同步的所述云计算平台中云资产信息的准确性，保证自动改密计划能正常执行；

S2 建立容错机制响应规则，建立在云计算平台中加入的容错机制响应规则，用于增加不同系统之间密码差异化，提升自动改密稳定性；其中，所述容错机制是指在云计算平台建立云堡垒机校验模块时，加入的自动改密容错机制；

S3 建立实时同步云计算平台中云资产信息的响应规则，建立在云计算平台中云资产信息动态交付和弹性伸缩等业务场景下的云计算平台中云资产信息的实时响应规则，实现所述云堡垒机和云计算平台的关于云计算平台中云资产信息实时自动同步；

S4 获取改密策略，获取云计算平台对自动改密自定义的计划任务，根据所述计划任务确定改密策略；

S5 执行自动改密，在获取自动改密策略后，云计算平台中自动调用步骤 S1 所对接的云计算平台与云堡垒机，完成所述云计算平台中云资产信息的自动改密策略的编排；自动响应步骤 S2 中的容错机制及所述云堡垒机校验模块并通过所述云堡垒机按照所述自动改密策略进行的定期自动校验及执行批量改密；并通过步骤 S3 将自动执行的结果由所述云堡垒机同步至所述云计算平台，并在对应的所述云主机中生效。

2、根据权利要求 1 所述的自动改密技术的方法，其特征还在于，

在所述步骤 S1 中，所述云堡垒机采用分布式架构，支持多机房跨区域部署，支持横向扩展，无云计算平台中云资产信息数量及并发限制；

所述云计算平台中云资产信息包含：云主机的 ip 及端口等基础信息、云租户的操作权限信息、云主机资源中管理员用户/非管理员用户的用户名和密码信息等多个账户的云资源账户信息；

所述云堡垒机作为云计算平台提供的服务之一提供给云租户，云租户通过云计算平台可直接跳转使用云堡垒机。

3、根据权利要求 1 或 2 所述的自动改密技术的方法，其特征还在于，

在所述步骤 S1 中，所述云堡垒机校验模块是，用于云计算平台定期自动或和云租户手动完成校验功能，在云计算平台中通过自动化技术完成对相关云主机云资产信息校验，通过

自动远程登入的方式验证其正确性，同时再与云堡垒机进行校验，保证云平台中云资产信息与云堡垒机中一致，当验证结果一致时，发起验证。

4、根据权利要求 1-3 任一项所述的自动改密技术的方法，其特征还在于，

在所述步骤 S2 中，所述自动改密容错机制包括：控制在自动改密任务执行的时候，同步逐条进行密码校验功能，在自动完成密码修改后，会记录之前的密码，再将新修改的密码一并记录；然后进行尝试自动的云主机新密码校验，若校验失败，则此条云主机任务回退，确保老密码可以登入；所有自动改密任务终止，需要人工介入，选择跳过或继续；若校验正确，则继续下一条任务。

5、根据权利要求 1 的自动改密技术的方法，其特征还在于，

在所述步骤 S3 中，所述动态交付和弹性伸缩等业务场景包括：通过云主机资源的动态伸缩，新伸展出来的云主机将具有独立的账号和密码，所述独立的账号和密码将与所述云堡垒机进行同步，以保证新生云主机资源的可操作性。

6、根据权利要求 1 的自动改密技术的方法，其特征还在于，

在所述步骤 S4 中，所述云计算平台对自动改密自定义的计划任务，包含：开始时间、涉及云主机清单、涉及云主机的使用者等。

7、一种面向云主机和云堡垒机实现含容错机制的自动改密的装置，其特征在于，包括：

部署并融合开源堡垒机模块，用于通过开源堡垒机自身的开放的 api 接口在云计算平台上构建了适合云业务场景的云堡垒机，实现云计算平台与云堡垒机的对接，及实现所述云计算平台的云资产信息与所述云堡垒机的云资产信息在云计算平台上进行统一管理和维护；同时在对接后的云计算平台上建立云堡垒机校验模块，用于确保在多云异构环境下，以验证和确保云计算平台与云堡垒机之间同步的所述云计算平台中云资产信息的准确性，保证自动改密计划能正常执行；

容错机制响应模块，用于自动响应容错机制的规则，用于增加不同系统之间密码差异化，提升自动改密稳定性；其中，所述容错机制是在云计算平台建立云堡垒机校验模块时，加入的自动改密容错机制；

实时同步云计算平台中云资产信息响应模块，用于自动响应在云计算平台中云资产信息动态交付和弹性伸缩等业务场景下的云计算平台中云资产信息的实时同步的规则，实现所述云堡垒机和云计算平台的关于云计算平台中云资产信息实时自动同步；

获取改密策略模块，用于获取云计算平台对自动改密自定义的计划任务，根据所述计划任务确定改密策略；

执行自动改密模块，用于在获取自动改密策略后，云计算平台中自动调用所述部署并融合开源堡垒机模块对接的云计算平台与云堡垒机，完成所述云计算平台中云资产信息的自动

改密策略的编排；自动所述容错机制响应模块中的容错机制及所述云堡垒机校验模块并通过所述云堡垒机按照所述自动改密策略进行的定期自动校验及执行批量改密；并通过所述实时同步云计算平台中云资产信息响应模块，将自动执行的结果由所述云堡垒机同步至所述云计算平台，并在对应的所述云主机中生效。

8、根据权利要求7的自动改密技术的装置，其特征还在于，
所述获取改密策略模块还包括：

显示子模块，用于显示云计算平台中专门用于云主机自动改密任务的模块的界面，可以提供用户自定义所需要启用自动改密的定时任务；

自定义改密策略子模块，云租户通过云计算平台可直接配置云资源改密计划，配置完成后得到自定义的自动改密策略。

9、一种电子装置，其特征在于，该装置包括存储器、处理器，所述存储器上存储有可在所述处理器上运行如权利要求7-8所述装置的配置程序，所述配置程序被所述处理器执行时可以实现如权利要求1-6所述的面向云主机和云堡垒机实现含容错机制的自动改密的方法。

10、一种计算机可读存储介质，其特征在于，所述计算机可读的存储介质上存储有权利要求7-8所述装置的配置程序，所述配置程序可以被一个或多个处理器执行，以实现如权利要求1-6所述的面向云主机和云堡垒机实现含容错机制的自动改密的方法。