(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102571895 A
(43)申请公布日 2012.07.11

(21)申请号 201110008700.1

(22)申请日 2011.01.17

(66)本国优先权数据
201010579734.1 2010.12.08 CN

(71)申请人 中国电信股份有限公司
地址 100032 北京市西城区金融大街 31 号

(72)发明人 江峰 雷葆华 张洁 蔡永顺
饶少阳 王峰 王志军

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 宋海宁

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
G06F 9/455(2006.01)

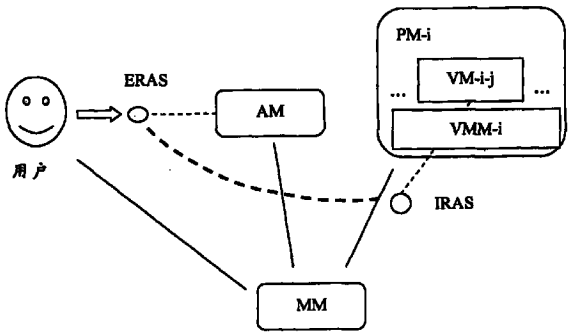
权利要求书 2 页 说明书 7 页 附图 2 页

(54)发明名称

远程访问虚拟机的方法和系统

(57)摘要

本发明提出远程访问虚拟机的方法和系统。当客户端发出远程访问虚拟机的请求时，管理模块查询到所要访问的虚拟机所处的物理机，通知物理机上运行的虚拟机管理器开放 IRAS；虚拟机管理器开放 IRAS，通知管理模块 IRAS，再由管理模块发送给访问接入模块；访问接入模块开放能被公网所访问的 ERAS，在 IRAS 和 ERAS 之间建立双向管道以传送数据；将 ERAS 返回给要访问虚拟机的客户端，客户端启动支持远程访问协议的客户端软件，访问 ERAS，经已建立的双向管道访问 IRAS，实现远程访问虚拟机。本发明隐藏了内网 IP、减少对公网 IP 地址数量的要求。



CN 102571895 A

1. 远程访问虚拟机的方法，包括：

当客户端发出远程访问虚拟机的请求时，管理模块查询到所要访问的虚拟机所处的物理机，通知所述物理机上运行的虚拟机管理器开放内部远程访问套接字；

虚拟机管理器开放内部远程访问套接字，通知管理模块所述内部远程访问套接字，再由管理模块发送给访问接入模块；

访问接入模块开放能被公网所访问的外部远程访问套接字，在内部远程访问套接字和外部远程访问套接字之间建立双向管道以传送数据；

将外部远程访问套接字返回给要访问虚拟机的客户端，客户端启动支持远程访问协议的客户端软件，访问外部远程访问套接字，经已建立的双向管道访问内部远程访问套接字，实现远程访问虚拟机。

2. 根据权利要求 1 所述远程访问虚拟机的方法，其中：

内部远程访问套接字为虚拟机所处的物理机的 IP 地址和端口号，外部远程访问套接字为公网的 IP 地址和端口号。

3. 根据权利要求 1 所述远程访问虚拟机的方法，其中，将外部远程访问套接字返回给要访问虚拟机的客户端的操作，包括：

由访问接入模块将外部远程访问套接字返回给要访问虚拟机的客户端，或者访问接入模块将外部远程访问套接字返回给管理模块，再由管理模块将外部远程访问套接字返回给要访问虚拟机的客户端。

4. 根据权利要求 1 所述远程访问虚拟机的方法，其中：客户端启动支持远程访问协议的客户端软件的操作，还包括：

输入认证信息，由虚拟机管理器根据在开放内部远程访问套接字时创建的认证信息进行比对，当输入的认证信息与之前创建的认证信息一致时，认证通过，访问外部远程访问套接字。

5. 根据权利要求 4 所述远程访问虚拟机的方法，其中：

当认证未通过时，访问接入模块延迟设定时间，将认证未通过信息返回给客户端，并限制同时访问同一个外部远程访问套接字的连接数。

6. 远程访问虚拟机的系统，包括：

物理机，运行着至少一台虚拟机；

虚拟机，运行在物理机上；

虚拟机管理器，运行在物理机上，对至少一台虚拟机进行管理；

管理模块，用于接收客户端的远程访问虚拟机的请求，查询所要访问的虚拟机所处的物理机，通知所述物理机上运行的虚拟机管理器开放内部远程访问套接字；获知虚拟机管理器开放的内部远程访问套接字，并通知给访问接入模块；

访问接入模块，用于开放能被公网所访问的外部远程访问套接字，在内部远程访问套接字以及外部远程访问套接字之间建立双向管道以传送数据；

客户端，用于向管理模块发出远程访问虚拟机的请求，在接收到外部远程访问套接字时，启动支持远程访问协议的客户端软件，访问外部远程访问套接字，经访问接入模块所建立的双向管道访问内部远程访问套接字，实现远程访问虚拟机。

7. 根据权利要求 6 所述远程访问虚拟机的系统，其中：

内部远程访问套接字为虚拟机所处的物理机的 IP 地址和端口号，外部远程访问套接字为公网的 IP 地址和端口号。

8. 根据权利要求 6 所述远程访问虚拟机的系统，其中：

访问接入模块将外部远程访问套接字返回给要访问虚拟机的客户端，或者访问接入模块将外部远程访问套接字返回给管理模块，再由管理模块将外部远程访问套接字返回给要访问虚拟机的客户端。

9. 根据权利要求 6 所述远程访问虚拟机的系统，其中：

虚拟机管理器在开放内部远程访问套接字时还创建认证信息，当客户端输入认证信息时，比对输入的认证信息与之前创建的认证信息是否一致，如果一致，认证通过。

10. 根据权利要求 9 所述远程访问虚拟机的系统，其中：

访问接入模块在认证未通过时，延迟设定时间，将认证未通过信息返回给客户端，并限制同时访问同一个外部远程访问套接字的连接数。

远程访问虚拟机的方法和系统

技术领域

[0001] 本发明属于计算机领域中的网络和虚拟化技术，尤其涉及远程访问虚拟机的方法和系统。

背景技术

[0002] 虚拟化技术是一种用软件模拟计算机硬件的技术，自从虚拟化技术获得了硬件厂商的支持以来，这种软件模拟硬件的性能获得了巨大的提升，以至于整个操作系统，例如Windows，不需要直接安装在物理硬件上，而是运行在虚拟硬件上，便可获得完全可以接受的性能。这种物理硬件称之为物理机 (Physical Machine，简称 PM)，而虚拟硬件称之为虚拟机 (Virtual Machine，简称 VM)，其上运行的操作系统称之为宾客操作系统 (Guest OS，简称 GOS)。管理虚拟机的软件称之为虚拟机管理器 (Virtual Machine Monitor，简称 VMM)。

[0003] 虚拟化技术带来的好处是明显的：因为它是软件模拟出来的，我们可以动态的调整虚拟机的性能。假设我们有一台配置很高的物理机，我们可以在这台物理机上创建多个虚拟机，并且可以让不同的虚拟机有不同的配置。对于占用计算机资源非常小的应用，我们可以只分配一个低配置的虚拟机；而对于占用计算机资源很大的应用，我们可以为其分配一个高配置的虚拟机。如果这个低配置的虚拟机的负载随着业务量的增加而变大时，我们可以动态的提高虚拟机的配置以满足性能的需求；而高配置的虚拟机的负载随着业务量的降低而变小时，我们可以动态的降低虚拟机的配置，从而把腾出来的计算资源分配给其他的虚拟机等等。这种动态的调整完全可以由软件来实现，例如部署一台预装了 Linux 操作系统的虚拟机只需要几分钟，而不是几个小时。

[0004] 有了虚拟化技术，IT 管理员只需要在个人电脑上进行一些操作就可以完成原本非常复杂的 IT 资源管理任务。此外，在虚拟机里面安装和运行操作系统，与在物理机中一模一样。即使一台物理机上同时运行着多个虚拟机，虚拟机的使用者也不知道它是在与别人分享一台物理计算机，甚至他根本就不知道他用的是物理机还是虚拟机。

[0005] 正因为上述好处，美国著名的亚马逊公司利用虚拟化技术将闲置的硬件服务器资源整合起来，形成一个虚拟的互联网数据中心 (Internet Data Center，IDC)，它颠覆了传统的 IDC 模式：人们通过亚马逊的网站就可以申请到一台虚拟机并开展互联网业务，例如架设自己的网站，而无须自己购买物理机，大大降低了初期 IT 投资成本。同时，虚拟机是按小时而不是按年按月收费的，例如我们只需要花几块钱就可以使用该虚拟机。

发明内容

[0006] 本发明提出远程访问虚拟机的方法和系统，让用户能够通过互联网访问即使出现严重故障的虚拟机，就好像用户“身临其境”的在机房内对他的物理机进行访问一样，看得见屏幕显示的内容，也可以用鼠标键盘对其进行控制。

[0007] 为了解决上述问题，本发明提出远程访问虚拟机的方法，包括：

[0008] 当客户端发出远程访问虚拟机的请求时，管理模块查询到所要访问的虚拟机所处

的物理机，通知所述物理机上运行的虚拟机管理器开放内部远程访问套接字；

[0009] 虚拟机管理器开放内部远程访问套接字，通知管理模块所述内部远程访问套接字，再由管理模块发送给访问接入模块；

[0010] 访问接入模块开放能被公网所访问的外部远程访问套接字，在内部远程访问套接字和外部远程访问套接字之间建立双向管道以传送数据；

[0011] 将外部远程访问套接字返回给要访问虚拟机的客户端，客户端启动支持远程访问协议的客户端软件，访问外部远程访问套接字，经已建立的双向管道访问内部远程访问套接字，实现远程访问虚拟机。

[0012] 本发明还提出远程访问虚拟机的系统，包括：

[0013] 物理机，运行着至少一台虚拟机；

[0014] 虚拟机，运行在物理机上；

[0015] 虚拟机管理器，运行在物理机上，对至少一台虚拟机进行管理；

[0016] 管理模块，用于接收客户端的远程访问虚拟机的请求，查询所要访问的虚拟机所处的物理机，通知所述物理机上运行的虚拟机管理器开放内部远程访问套接字；获知虚拟机管理器开放的内部远程访问套接字，并通知给访问接入模块；

[0017] 访问接入模块，用于开放能被公网所访问的外部远程访问套接字，在内部远程访问套接字以及外部远程访问套接字之间建立双向管道以传送数据；

[0018] 客户端，用于向管理模块发出远程访问虚拟机的请求，在接收到外部远程访问套接字时，启动支持远程访问协议的客户端软件，访问外部远程访问套接字，经访问接入模块所建立的双向管道访问内部远程访问套接字，实现远程访问虚拟机。

[0019] 与现有技术相比，本发明让用户能够通过互联网访问即使出现严重故障的虚拟机，就好像用户“身临其境”的在机房内对他的物理机进行访问一样，看得见屏幕显示的内容，也可以用鼠标键盘对其进行控制。还隐藏了内网 IP、减少对公网 IP 地址数量的要求。

[0020] 本发明还由虚拟机管理器在开放内部远程访问套接字时还创建认证信息，当客户端输入认证信息时，比对输入的认证信息与之前创建的认证信息是否一致，如果一致，认证通过。从而，利用预设或临时设定的认证信息来确保只有合法用户才能访问虚拟机。

[0021] 本发明还由访问接入模块在认证未通过时，延迟设定时间，将认证未通过信息返回给客户端，并限制同时访问同一个外部远程访问套接字的连接数。从而，保护利用两次访问间的时间间隔、限制同时最大连接数的方式防止攻击。

附图说明

[0022] 图 1 为本发明远程访问虚拟机的系统结构图。

[0023] 图 2 为本发明远程访问虚拟机的方法流程图。

具体实施方式

[0024] 在传统的 IDC 运营模式下，如果用户托管在机房的物理机出现严重故障，例如，在操作系统根本无法正常的引导、更谈不上远程登录到该计算机的情况下，那么，用户可以亲自到机房现场对他的物理机进行故障排查。但是，在虚拟 IDC 中，用户的计算机是虚拟机，不是一个摸得着看得见的机器。即使可以定位到具体的某台物理机，但是该物理机上可能

运行着其他用户的虚拟机。因此，让用户到机房来排查故障是不现实的方法。

[0025] 本发明的目的是让用户能够通过互联网访问即使出现严重故障的虚拟机，就好像用户“身临其境”的在机房内对他的物理机进行访问一样，看得见屏幕显示的内容，也可以用鼠标键盘对其进行控制。

[0026] 下面将结合附图对本发明的实现过程进行详细说明。

[0027] 如图 1 所示，有 n 个物理机 PM-1，PM-2，...，PM-n，其中 PM-i 表示第 i 台物理机。在每台物理机上运行着至少一台虚拟机。

[0028] 虚拟机 VM，运行在物理机上，其中 VM-i-j 表示在第 i 台物理机上运行的第 j 台虚拟机。

[0029] 虚拟机管理器 VMM，运行在物理机上，对至少一台虚拟机进行管理。

[0030] 管理模块，简称 MM，它管理或协调着所有的 PM、VMM、VM、AM。用于接收客户端的远程访问虚拟机的请求，查询所要访问的虚拟机所处的物理机，通知所述物理机上运行的虚拟机管理器开放内部远程访问套接字 (Internal Remote Access Socket，IRAS) ；获知虚拟机管理器开放的内部远程访问套接字，并通知给访问接入模块。其中，内部远程访问套接字为虚拟机所处的物理机的 IP 地址和端口号。

[0031] 访问接入模块，简称 AM。用于开放能被公网所访问的外部远程访问套接字 (External Remote Access Socket，ERAS)，在内部远程访问套接字以及外部远程访问套接字之间建立双向管道以传送数据。其中，外部远程访问套接字为公网的 IP 地址和端口号。

[0032] 作为本发明的一个实施例，访问接入模块将外部远程访问套接字返回给要访问虚拟机的客户端，或者访问接入模块将外部远程访问套接字返回给管理模块，再由管理模块将外部远程访问套接字返回给要访问虚拟机的客户端。

[0033] 客户端，用于向管理模块发出远程访问虚拟机的请求，在接收到外部远程访问套接字时，启动支持远程访问协议的客户端软件，访问外部远程访问套接字，经访问接入模块所建立的双向管道访问内部远程访问套接字，实现远程访问虚拟机。

[0034] 本发明中，访问接入模块充当着 IRAS 和 ERAS 之间的双向管道，虽然，用户获得的是 ERAS 不是 IRAS，但通过访问接入模块的双向传送，客户端软件实际上是与 IRAS 通讯。这样，用户既可以利用远程访问协议通过虚拟机管理器访问虚拟机，也使得整个系统无须暴露 PM 的 IP 地址，可以提高安全性。也不要求每个 PM 有独立的公网 IP (客户端只是访问 ERAS 而已)，减少了对公网 IP 的占用量。

[0035] 进一步，由于用户在安装虚拟机的时候设有密码，那么，管理模块接收客户端的远程访问虚拟机的请求，在请求中还包括用户名、用户密码和虚拟机。管理模块根据用户名和用户密码来验证用户是否为假冒的。在设置密码后，至少只有虚拟机的主机才能接触到这台虚拟机，至于是不是能登陆虚拟机，还得看此人是否有虚拟机操作系统的帐号了。所以，在通过用户名和用户密码验证后，管理模块还要根据用户名和虚拟机来判断用户是否有权限访问这个虚拟机。从而确保用户不能访问别人的虚拟机。在执行上述验证过程之后，管理模块查询所要访问的虚拟机所处的物理机。

[0036] 进一步，虚拟机管理器在开放内部远程访问套接字时还创建认证信息，当客户端启动支持远程访问协议的客户端软件时，输入认证信息，由虚拟机管理器比对输入的认证信息与之前创建的认证信息是否一致，如果一致，认证通过。本发明虚拟机管理器可以利用

预设或临时设定的认证信息来确保只有合法用户才能访问虚拟机。

[0037] 进一步，虚拟机管理器还将认证结果通过管理模块发送给访问接入模块，当认证通过时，访问接入模块通知客户端，客户端可以访问外部远程访问套接字。当认证未通过时，虚拟机管理器将会关闭 IRAS，拒绝访问。访问接入模块延迟设定时间，将认证未通过信息返回给客户端，并限制同时访问同一个外部远程访问套接字的连接数。本发明可以保护利用两次访问时间的间隔、限制同时最大连接数的方式防止攻击。

[0038] 结合图 2 中远程访问虚拟机的方法流程，对上述各部分所执行的操作进行说明，具体包括以下步骤：

[0039] 在步骤 201，当客户端发出远程访问虚拟机的请求时，管理模块查询所要访问的虚拟机所处的物理机，通知所述物理机上运行的虚拟机管理器开放内部远程访问套接字，如果该端口没有被开放的话。其中，内部远程访问套接字为虚拟机所处的物理机的 IP 地址和端口号。

[0040] 作为本发明的一个实施例，当客户端发出远程访问虚拟机的请求的操作是：例如点击网页上的某个 URL，服务器收到访问请求之后会识别这个 URL 的含义，这里所说的服务器是指承载网站的应用服务器，注入 WebLogic、Tomcat 等。如果发现是发起访问请求，则将访问请求交给 MM，此时，MM 会根据该 URL 得知用户希望访问的虚拟机。

[0041] 作为本发明的一个实施例，管理模块查询虚拟机所处的物理机的操作中，还可以根据以下信息执行具体操作：用户名、用户密码、虚拟机。首先，由于用户在安装虚拟机的时候设有密码，那么，在用户要访问虚拟机时，管理模块根据用户名和用户密码来验证用户是否为假冒的。在设置密码后，至少只有虚拟机的主机才能接触到这台虚拟机，至于是不是能登陆虚拟机，还得看此人是否有虚拟机操作系统的帐号了。所以，在通过用户名和用户密码验证之后，管理模块还要根据用户名和虚拟机来判断用户是否有权限访问这个虚拟机。从而确保用户不能访问别人的虚拟机。如果有权限访问虚拟机，则管理模块查询虚拟机所处的物理机。

[0042] 作为本发明的一个实施例，通知物理机上运行的虚拟机管理器开放内部远程访问套接字的操作中，不必指定监听端口。管理模块发出请求，虚拟机管理器就会开放一个端口，然后把端口号返回给管理模块。这样管理模块就知道虚拟机管理器已经成功开放端口了。

[0043] 在步骤 202，虚拟机管理器开放内部远程访问套接字，通知管理模块所述内部远程访问套接字，再由管理模块发送给访问接入模块。

[0044] 在步骤 203，访问接入模块开放能被公网所访问的外部远程访问套接字，在内部远程访问套接字和外部远程访问套接字之间建立双向管道以传送数据。其中，外部远程访问套接字为公网的 IP 地址和端口号。

[0045] 假设该外部远程访问套接字 ERAS 的 IP 地址是 IP-i-j，其端口号是 PORT-i-j。从此时开始，AM 就充当着 IRAS 和 ERAS 之间的双向管道，负责两边的数据转发，直到任何一方关闭或出现异常情况。

[0046] 在步骤 204，将外部远程访问套接字返回给要访问虚拟机的客户端，客户端启动支持远程访问协议的客户端软件，访问外部远程访问套接字，经已建立的双向管道访问内部远程访问套接字，实现远程访问虚拟机。

[0047] 作为本发明的一个实施例，将外部远程访问套接字返回给要访问虚拟机的客户端的操作，包括：由访问接入模块将外部远程访问套接字返回给要访问虚拟机的客户端，或者访问接入模块将外部远程访问套接字返回给管理模块，再由管理模块将外部远程访问套接字返回给要访问虚拟机的客户端。

[0048] 客户端直接与虚拟机管理器打交道，虚拟机管理器是装在物理机上，所以不依赖虚拟机操作系统是否正确的启动了。换句话说，不论虚拟机操作系统是否正确的启动，那么本应该显示在显示器上的视频信息都会传到客户端。用户也可以通过客户端发出键盘、鼠标事件，对这个虚拟机进行操作。就好像用户“身临其境”的在机房进行操作一样。

[0049] 作为本发明的一个实施例，还可以进一步保证只有授权的用户才能访问虚拟机，在上述方法流程之上采取进一步的措施为：

[0050] 在步骤 201 中，虚拟机管理器开放内部远程访问套接字 IRAS 时，会根据 MM 或系统其他模块提供的认证信息来创建认证信息，或者用户临时将认证信息传给 MM，再由 MM 传给 VMM 要求其修改远程访问的认证信息，并由 VMM 创建认证信息。

[0051] 在步骤 204，客户端启动支持远程访问协议的客户端软件的操作，还包括：输入认证信息，由虚拟机管理器将在开放内部远程访问套接字时创建的认证信息与输入的认证信息进行比对，将比对结果通过管理模块发送给访问接入模块。该认证信息可以是预设或临时设定的密码，或者其他不被第三方所知的信息。这样提高了使用的安全性。

[0052] 进一步，在步骤 204 中，当输入的认证信息与之前创建的认证信息一致时，认证通过，访问接入模块通知客户端认证通过，客户端可以访问外部远程访问套接字。当认证未通过时，虚拟机管理器将会关闭 IRAS，拒绝访问。访问接入模块延迟设定时间，通知客户端认证未通过，并限制同时访问同一个外部远程访问套接字的连接数。防止非法用户采用字典攻击等手段猜测并伪造认证信息。

[0053] 下面通过具体实施例，对本发明的实现过程进行说明。

[0054] 在该实施例中，整个系统包括虚拟机管理器 (VMM)、虚拟机 (VM)、宾客操作系统 (GuestOS)、访问接入模块 (AM) 以及管理模块 (MM)。其中 VMM 采用基于内核的虚拟机 (Kernel-based Virtual Machine，KVM)，宾客操作系统采用 Windows 2008。

[0055] 在正常情况下，GuestOS 应该获得一个公网 IP 地址，用户可以根据 RDP 协议 (Remote Desktop Protocol，远程桌面访问协议）通过该公网 IP 地址访问该 GuestOS。

[0056] 但是，GuestOS 出现严重故障，例如 Windows 2008 无法被正常引导时，用户无法访问系统以进行故障排查，因此类似于 RDP 的方法就是无效的。这时，用户需要一种更好的方法使其仍然可以通过互联网访问并控制他的虚拟机。这就是本发明所提出的方法。

[0057] 在 MM 要求 KVM 启动一个 VM 时，会在启动参数中增加一个指定 VNC 的监听端口的参数，例如“-vnc:1”。那么在 KVM 启动一个 VM 时，一个用于 VNC 连接的内部远程访问套接字就会被打开，其监听端口号为 5901，其监听的 IP 地址为 VM 所在的物理机的 IP 地址，例如 192.168.0.1。

[0058] 在 KVM 启动一个 VM 后，KVM 会立即设置一个 VNC 访问密码，该密码可以是随机设定或者用户预先设定好的。

[0059] 当用户发出远程访问该虚拟机 VM 的请求时，MM 会查询到该 VM，并获得用于 VNC 的套接字的 IP 地址与端口号，如 192.168.0.1:5901。

[0060] MM 将该内部远程访问套接字的 IP 地址与端口号告诉 AM，AM 会开放一个能被公网所访问的外部远程访问套接字，例如 100.100.0.1:5000。AM 会在内部远程访问套接字 (192.168.0.1:5901) 以及新建立的外部远程访问套接字 (100.100.0.1:5000) 之间建立一个双向管道，将所有从前者读取的数据转发给后者，同时也将所有从后者读取到的数据转发给前者。任何一端关闭或者出现异常，AM 都会通知另一方后关闭连接。

[0061] AM 把新创建的外部远程访问套接字信息 (100.100.0.1:5000) 告诉 MM，MM 会将这个信息传给用户。

[0062] 客户端启动一个 VNC 客户端软件。如果访问密码是随机设定的，客户端软件将访问密码传给 MM，由 MM 传给 KVM 并让其重新设定 VNC 的访问密码。因为用户使用 VNC 客户端来访问 KVM，虽然中间通过了 AM，但 AM 只是负责转发数据包，并未参与数据内容。而访问 VNC 是需要密码的。所以让用户自己在发出请求的时候，临时填一个访问密码作为请求的一部分发给 MM。只有知道这个临时密码的用户才能接入 VNC。如果访问密码是用户预先设定好的，当用户访问外部远程访问套接字 (100.100.0.1:5000) 时，VNC 客户端会提示用户输入密码。如果用户不能输入正确的密码，将无法访问虚拟机。

[0063] 当 KVM 通过 AM 向客户端返回认证未通过信息的时候，AM 将该认证未通过信息延迟一段时间再返回给客户端，AM 还限制同时访问同一个外部远程访问套接字 (100.100.0.1:5000) 的连接不能超过 3 个。其中，延迟发送认证未通过信息的目的是，比如，如果不做任何延迟，那么非法者可以一秒钟探测 100000 次。但如果延迟一秒，非法者一秒钟最多探测一次。这就限制了探测的频率，增加了探测的难度，也就有效的防止了非法用户采用字典攻击等手段猜测并伪造认证信息。

[0064] 当 KVM 通过 AM 向客户端返回认证通过信息的时候，客户端访问外部远程访问套接字 (100.100.0.1:5000)，由于 AM 的转发，因此客户端访问的其实是内网的内部远程访问套接字 (192.168.0.1:5901)。至此，客户端就可以远程访问内网里面的虚拟机了。

[0065] 上述方法达到的效果是 :用户是通过访问一个公网 IP 地址来间接访问虚拟机的，而无须直接访问虚拟机所在的物理机 IP。因此，隐藏内网 IP、大大降低了对公网 IP 数量的要求。进一步，本发明利用预设或临时设定的认证信息来确保只有合法用户才能访问虚拟机。进一步，保护利用两次访问间的时间间隔、限制同时最大连接数的方式防止攻击。

[0066] 将会理解，在一个实施例中，所讨论的方法步骤是由执行存储在存储装置中的指令（代码段）的处理（即计算机）系统的（一个或多个）适当的处理器来执行的。还将理解，本发明并不局限于任何特定的实现方式或编程技术，并且本发明可以用任何适当的用于实现这里所描述的功能的技术来实现。本发明并不局限于任何特定的编程语言或操作系统。从而，正如本领域的技术人员将会意识到的，本发明的实施例可以实现为方法、诸如专用装置这样的装置、诸如数据处理系统这样的装置，或者承载介质，例如计算机程序产品。承载介质承载用于控制处理系统实现方法的一个或多个计算机可读代码段。因此，本发明的方面可以采取方法、纯硬件实施例、纯软件实施例或者结合了软件和硬件方面的实施例的形式。此外，本发明可以采取承载包含在介质中的计算机可读程序代码段的承载介质（例如计算机可读存储介质上的计算机程序产品）的形式。可以使用任何合适的计算机可读介质，其中包括诸如磁盘或硬盘这样的磁存储设备，或者诸如 CD-ROM 这样的光存储介质。

[0067] 作为对详细描述的结论，应该注意本领域的技术人员将会很清楚可对优选实施例做出许多变化和修改，而实质上不脱离本发明的原理。这种变化和修改包含在所附权利要求书所述的本发明的范围之内。

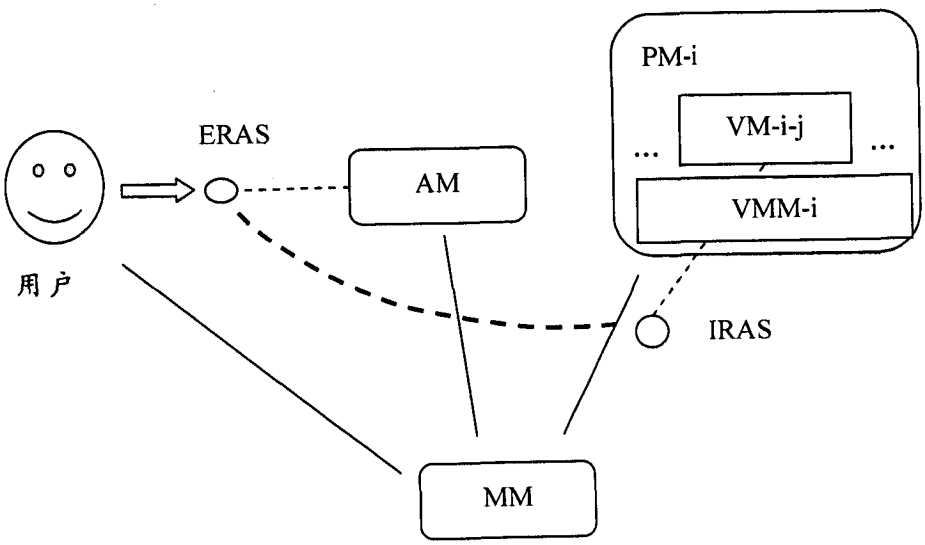


图 1

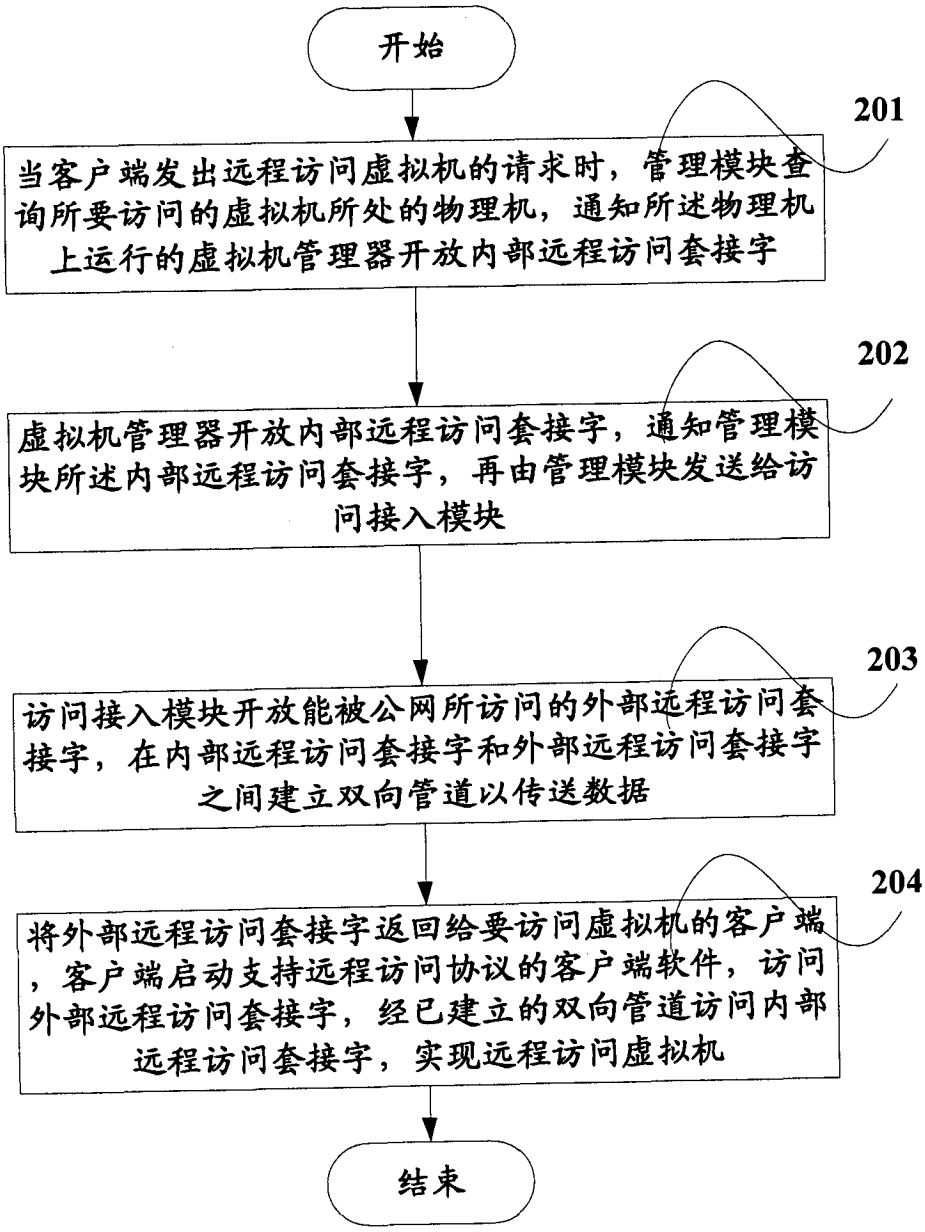

开始
201
当客户端发出远程访问虚拟机的请求时，管理模块查询所要访问的虚拟机所处的物理机，通知所述物理机上运行的虚拟机管理器开放内部远程访问套接字
202
虚拟机管理器开放内部远程访问套接字，通知管理模块所述内部远程访问套接字，再由管理模块发送给访问接入模块
203
访问接入模块开放能被公网所访问的外部远程访问套接字，在内部远程访问套接字和外部远程访问套接字之间建立双向管道以传送数据
204
将外部远程访问套接字返回给要访问虚拟机的客户端，客户端启动支持远程访问协议的客户端软件，访问外部远程访问套接字，经已建立的双向管道访问内部远程访问套接字，实现远程访问虚拟机
结束

图 2