基于虚拟组织的桌面云安全访问与共享机制研究

陈伟[1]，曹军威[1,2]，钱瀚[3]

（1. 清华大学信息技术研究院，北京 100084；
2. 清华信息科学技术国家实验室，北京 100084；
3. 清华大学自动化系，北京 100084）

摘 要：采用云计算技术实现托管式的虚拟桌面一般被称为桌面云。近年来桌面云被认为是云计算最为成熟的应用之一，本文着重研究桌面云安全访问与共享机制。我们使用基于 PKI 的证书认证建立了虚拟组织，在其上重点研究了虚拟机的创建，远程桌面访问，共享等应用。证书认证等机制可以使得访问更加安全可靠。而通过虚拟组织的信任关系，多个用户可以共享同一个虚拟机。为了确保远程通道的安全，我们采用了 OpenVPN 来构建虚拟专用网络，对虚拟机的使用者进行认证并对通信进行加密保护。

关键字：虚拟组织；虚拟机；桌面云；安全访问与共享

Virtual organization based secure accessing and sharing in desktop clouds

CHEN Wei[1], *CAO Jun-wei*[1,2], *QIAN Han*[3]

(1. Research Institute of Information Technology, Tsinghua University, Beijing 100084, China;
2. Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China;
3. Department of Automation, Tsinghua University, Beijing 100084, China)

Abstract: A desktop cloud is an implementation of hosted virtual desktops using cloud computing technology. Desktop clouds are one of the most popular applications for cloud computing. In this work, mechanisms for secure accessing and sharing of virtual desktops are investigated in details. The public key infrastructure (PKI) is utilized to create virtual organizations (VO). Within a VO, virtual machines are created, remote desktops are accessed and shared. PKI provides security mechanism and multiple users can share a virtual machine via VO trust management. In order to make remote channels secure, OpenVPN is adopted to build a private network, authenticating users and encrypting communications.

Key words: virtual organizations; virtual machines; desktop clouds; secure accessing and sharing

---

收稿日期：2012-11-10；修回日期：2012-11-10。
基金项目：国家自然科学基金委项目（61233016）；国家 973 计划资助项目（2011CB302805）。
作者简介：陈伟，男，硕士研究生，研究领域为虚拟化与云计算；曹军威（1973- ），男，清华大学信息技术研究院研究员，研究方向为先进计算技术与应用，E-mail: jcao@tsinghua.edu.cn. 钱瀚，男，本科生，研究方向为虚拟机安全访问与共享。

引言

云计算是当前计算机领域最为热门的问题之一，可以通过计算资源的虚拟化技术，打破数据中心服务器的物理限制，实现弹性的资源提供，以及按需的平台和软件服务[1]。云计算的发展符合计算技术基础架构化的大趋势，是继网格计算、服务计算之后兴起的又一轮技术创新和产业化热潮[2]。

云计算的一个重要应用场景就是桌面云。远程桌面的技术由来已久，而桌面云是近年来兴起的将远程桌面与云计算技术相结合的产物。IBM 对其做出的定义为：“可以通过瘦客户端或者其他任何与网络相连的设备来访问跨平台的应用程序，以及整个客户桌面”[3]。通过云计算平台来托管多个用户或应用的虚拟机，不同平台下的用户主机或者应用服务器可以进一步共享云平台的资源，同时支持用户通过远程桌面在线访问[4]。

随着网络的不断发展，人们有条件采用图形化的方式来访问远程的资源，因此瘦客户端的模式[5][6]很早就引起了研究者的关注。在目前大量的远程图形化访问协议中，微软的 RDP **错误!未找到引用源。**，开源的 VNC **错误!未找到引用源。**，Citrix 的 ICA[9]协议是目前应用比较广泛的。RDP 协议仅能用于 windows 系统之间的远程连接，但 linux 系统上有开源的 rdesktop 实现，可以作为 RDP 的客户端。VNC 协议则是开源的，在各种系统上均能够使用，但由于传送的数据量比较大，在网络和终端处理能力有限的情况下表现不佳。

本文实现了一个桌面云的安全访问和共享管理系统。相比于传统的远程桌面访问软件，本系统更加注重用户之间的关系，采用虚拟组织的方式对所有的用户及资源进行组织管理。同时通过 VPN 等技术与 RDP 远程访问相结合，确保访问的安全性。虚拟组织[10]，是通过虚拟的信息来组织人或其他资源之间的关系。在云计算中，离不开各个用户之间的关系，也离不开人对资源的占有和共享。因此在云计算中采用虚拟组织的形式来组织用户关系是一种有效的尝试。

本文第 1 章开始介绍虚拟组织的认证与管理，第 2 章为基于虚拟组织的桌面云中虚拟机的管理和共享机制研究，第 3 章阐述虚拟机的安全访问机制，第 4 章是系统的实现以及使用案例。

1 虚拟组织认证与管理

虚拟组织（Virual Organization），又称虚拟社区（Virtual Community），可以定义为一群主要藉由计算机网络彼此沟通的人们，他们彼此有某种程度的认识、分享某种程度的知识和信息、在很大程度上如同对待朋友般彼此关怀，从而所形成的团体。

虚拟组织拥有不同于现实社区的独特属性：

超时空性：虚拟组织不受物理上距离的限制，地球两端的两个人也可以通过虚拟组织进行交流。时间上也同样不受限制，你所发表的一句话或是一个操作，可能会在几天后被其他人看到并作出回应。

匿名性：在虚拟组织中每个人都只有一个符号。你可以随意选取你的名字，由于不能看到对方的真面目，传统的性别，年龄，相貌，都在虚拟组织里不再重要。

群体流动频繁：在虚拟组织中，人际关系较为松散，群体流动频繁，大家可能会被某个组织的人气所吸引而加入一个组织。

1. 1 成员身份认证

虚拟组织的管理基于用户身份认证和数据库的查询与更新。对此我们采用了相对比较成熟的认证机制和数据库管理软件，以保证系统的安全性和可靠性。

身份认证基于数字证书 PKI 机制。PKI（Public Key Infrastructure）即“公钥基础设施”，“是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。”[11][12]

PKI 允许用户相互验证各自使用的、由认证中心颁发的数字证书，从而确认对方身份并建立加密可信的连接。

1.2 组织管理

虚拟组织的管理主要通过虚拟组织的中心服务器实现。中心服务器在整个系统中起了核心的作用，负责了所有用户和资源信息的存储，以及用户间，用户与资源间的信息交互。它主要由两部分程序组成：一是等待用户传送信息并处理，二是发送请求到服务提供商。在我们的虚拟机远程访问的应用中，服务提供商就是虚拟机的管理端。

接受用户的信息端，服务器接受到客户端发送的请求后，仍然是分为两种情况，一种是虚拟组织操作命令，另一种是虚拟机相关操作命令。

对于虚拟组织操作命令，主要包括创建虚拟组织，删除虚拟组织，申请加入，批准成员加入，从组织中删除成员等。这部分命令和逻辑是基于虚拟组织的服务通用的。

2 虚拟机管理与共享机制

基于虚拟组织的成员认证和管理，可以实现桌面云中虚拟机的管理与共享。下面分别介绍桌面云应用中用户的几种主要请求情况。

2.1 新建虚拟机

在我们的系统中，同一个虚拟组织内部可以深度共享资源，因此虚拟机在虚拟组织内是可以共享的。而一个用户可以加入多个虚拟组织，并使用这几个虚拟组织中的虚拟机。因此用户在要求新建虚拟机的时候必须指定将该虚拟机共享于哪一个虚拟组织内。

在客户端的设计中，用户此时发送的信息包括：

事件：CreateVM（创建虚拟机）虚拟组织名称：VoName 设计虚拟机名称： VmName。

创建虚拟机的流程包括：1. 检查用户身份。2. 检查虚拟组织即确认权限。 3. 查找可用的虚拟机提供端。4. 向虚拟机提供端提交请求。5. 向数据库中添加记录。

2.2 开启虚拟机

在客户端的设计中，开启虚拟机发送的信息包括：

事件：OpenVm 虚拟机名称：VmName

在创建虚拟机的时候，虚拟机名称就已经确定了，而且是唯一的，因此用户只需要指定虚拟机的名称就可以了。

服务器在接收到指令之后，进行以下步骤。1. 检查用户身份。2. 在数据库中查询用户所在的虚拟组织。3. 找到用户所请求的虚拟机，未授权的虚拟机则无法查询到。4. 向虚拟机提供端提交请求。5. 将虚拟机访问信息返回给用户。

2.3 关闭（休眠）虚拟机

关闭虚拟机是比较简单的一个步骤，基本与开启虚拟机相同。只不过发送的指令是：

事件：CloseVm(SleepVm) 虚拟机名称：VmName

其后的操作与开启虚拟机基本对应。

3 虚拟机安全远程访问

我们使用 VirtualBox 提供虚拟机支持[13][14]，同时 VirtualBox 虚拟机本身支持开启 RDP 远程桌面的功能，我们正是利用这个特性进行虚拟机的远程访问。在服务端，开启虚拟机时使用 VBoxHeadless 命令，就可以让虚拟机在后台打开，并且在宿主机中的某一个端口开启基于 TCP 协议的 RDP 服务。

在客户端可以使用 rdesktop[15]命令来远程访问该虚拟机。然而，VirtualBox 中的 RDP 协议仅有不进行认证和进行简单认证两种方式来控制终端的连接，从安全访问的角度来讲这是远远不够的。因此，我们使用了 VPN 来保证访问的安全性和唯一性。

VPN（Virtual Private Network），即虚拟专用网络。目前组建 VPN 虚拟专用网主要依靠四项技术来保证安全：隧道技术、加解密技术、密钥管理技术和身份认证技术[16][17]。在本工作中，我

们用 OpenVPN 对证书的验证功能。

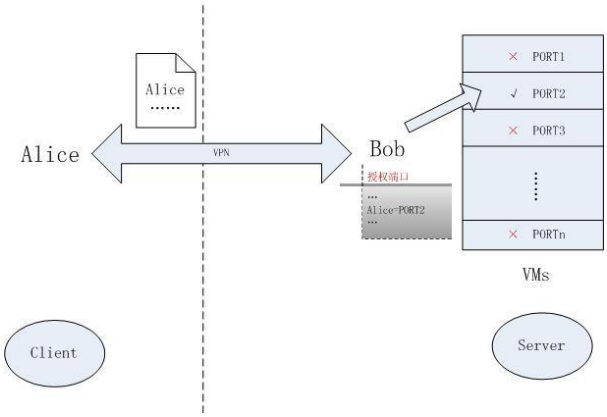

图 1　防火墙和授权远程访问实现

整个系统分为客户端和服务器端，效果如图 1 所示。在上图中，客户端指的是远程访问使用的显示终端，服务器端指的是虚拟机提供桌面云端。服务器在云计算中可以是提供虚拟资源的服务器集群，在虚拟组织内每位提供虚拟机共享的成员都可以作为服务器。由于 VirtualBox 的访问模式是主机的域名（或 IP）加上被访问虚拟机占用的主机端口，虚拟机访问权限的控制就可以简化为对服务器端口访问的控制。

防火墙开启后，所有虚拟机所占用的端口都被保护，不能被访问。如何开启某端口的访问权限，这需要 OpenVPN 的配合。

首先在服务器上安装 OpenVPN，使用 OpenVPN 进行身份验证需要 CA 的公钥和 CA 颁发给用户的证书，在配置文件中设置公钥证书的访问路径。OpenVPN 配置完毕后开启 OpenVPN 服务，客户端就可以与服务器端建立安全连接。

需要注意的是，并不是所有的证书验证通过就能获得端口访问权限，证书验证通过只能说明对方与自己来自同一个组织，这里需要增加用户访问端口的权限。读取证书后获得证书 CN(common name)，使用 CN=PORT 的格式添加使用权限，如授权成员 Alice 端口 3399 的访问权限，就可以在/etc/openvpn/clients.rc 添加 Alice=3399。

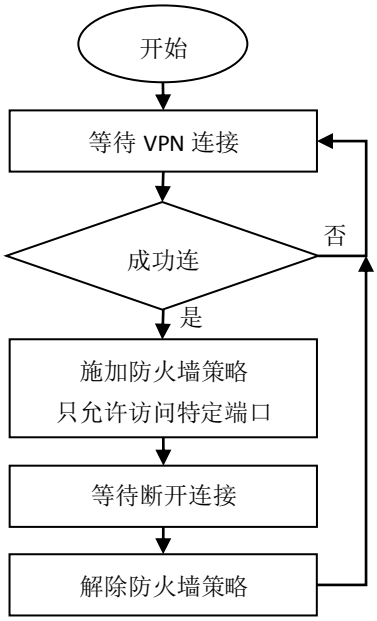

图 2　服务器端流程图

4 系统实现与使用案例

4. 1 虚拟机管理与共享

客户端目前采用命令行的方式与虚拟组织服务器交互。看一下多个用户在虚拟组织的管理之下的一些特性。

如图 3 所示，用户 alice 首先使用 setupVO 创建一个虚拟组织，名称为 VO1，并且为其添加了一个虚拟机 alice_1。

用户 alice 就可以成功访问虚拟机 alice_1 并且打开远程桌面进行使用。

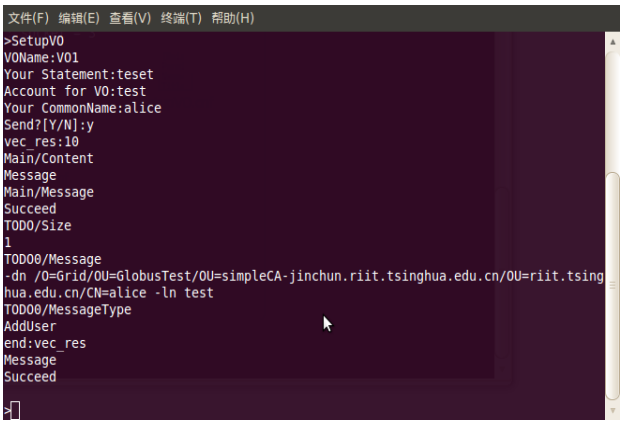

图 3　用户 alice 创建虚拟组织与虚拟机

我们保留 alice 建立的虚拟组织，然后使用另一个用户 bob 登陆客户端，首先他尝试打开 alice 建立的虚拟机，系统将会返回错误信息，因为 bob 不属于 alice 建立的那个虚拟组织，无法使用该虚拟机。系统错误信息指出用户 bob 和 alice 创建的虚拟机 alice_1 不属于同一个 VO，因此访问不成功。虚拟组织的管理起到了资源和用户之间的全局权限管理的作用。

Bob 此时申请加入 VO1，提交申请后使用 alice 登录批准该申请（因为 alice 是 VO1 的管理员），再次用 bob 登录，此时 bob 已经是 VO1 组织中的正式成员，再次尝试开启虚拟机则可以成功，如图 4。

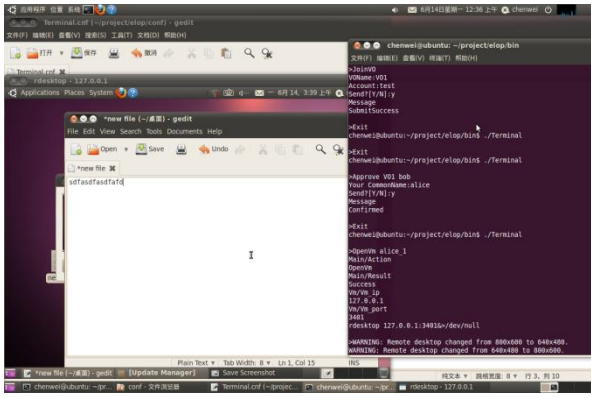

图 4 用户 bob 加入 VO1 后成功访问虚拟机 alice_1 并且打开远程桌面

上述实验说明，在虚拟组织的管理下，用户可以创建，开启虚拟机，并选择在什么情况下共享该虚拟机。实现了在用户间资源的深度共享。

4. 2 虚拟机安全访问

由于 VirtualBox 中的身份认证十分简单，而其官方文档也建议将此认证仅仅作为试用的认证方式。因此我们设置在 VirtualBox 中对用户身份不认证，而如何确保安全访问由 VPN 来控制。

我们在服务器端开启两台虚拟机，操作系统分别为 Windows XP 和 Ubuntu，占用主机端口分别为 3389 和 3391。然后开启防火墙和 OpenVPN 服务，等待客户端的连接。

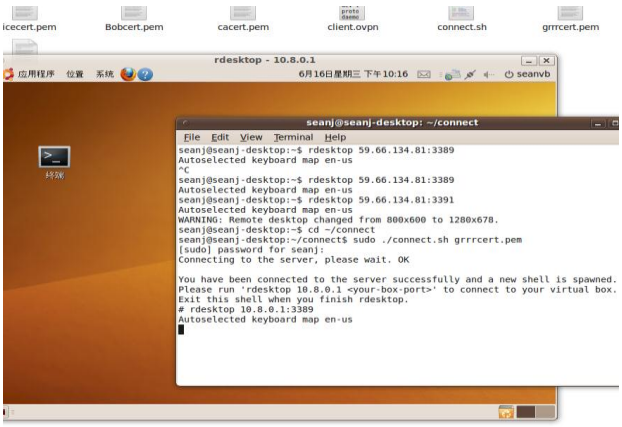

图 5 使用授权证书访问虚拟机

客户端使用 CA 服务器颁发的证书去连接虚拟组织服务器，如果服务器的端口访问控制策略里授权该用户使用某端口，则可以访问该端口，即可以远程控制该端口的虚拟机。

本例中服务器为证书 grrrcert.pem 授权了端口 3389 和 3391，所以可以使用 rdesktop 连接 10.8.0.1 的 3389 端口。客户端与服务器主机之间建立的安全通道，服务器端被定义为 10.8.0.1 这一虚拟 IP，使用服务器真实 IP 连接则被防火墙拒绝。

```
# exit
Disconnecting...  Done
seanj@seanj-desktop:~/connect$ sudo ./connect.sh alicecert.pem
Connecting to the server, please waitEnter Private Key Password:
. OK

You have been connected to the server successfully and a new shell is spawned.
Please run 'rdesktop 10.8.0.1 <your-box-port>' to connect to your virtual box.
Exit this shell when you finish rdesktop.
# rdesktop 10.8.0.1:3389
Autoselected keyboard map en-us
# rdesktop 10.8.0.1:3391
Autoselected keyboard map en-us
ERROR: 10.8.0.1: unable to connect
#
```

图 6 使用证书访问未授权的虚拟机不成功

如图 6 所示，服务器为 alicecert.pem 授予 3389 端口的使用权限，alicecert.pem 可以正常访问该端口的虚拟机，但是对于未授权的 3391 端口则会被服务器拒绝，尽管此时 3391 端口已经为用户 grrrcert.pem 开放。

至此可以发现，使用防火墙和 OpenVPN 使虚拟机的共享安全和可靠，即控制了访问权限，又保证了数据传送的安全。

总结

本工作选取了远程虚拟机访问这一云计算中的关键问题来进行研究。虚拟组织是在虚拟环境

下对用户关系的一种模拟，可以很好的建立用户之间数据，资源共享机制，并且具有良好的可扩展性。在虚拟组织的基础上，我们实现了虚拟机的远程申请，访问，关闭，共享等功能，是针对虚拟组织应用的一个扩展，也是未来云计算虚拟化管理的重要方向。在虚拟机远程访问中，安全性是一个重要的问题，我们采用 VPN 这样一种成熟的协议来确保访问的安全，具有更好的可靠性和可移植性。

本工作未来具有广阔的应用前景，比如云制造是未来面向服务的网络化制造新模式[18]，在云制造应用中，制造业的仿真和设计需要特殊的软件和海量的计算资源做支持，云计算是理想的模式。未来工作将主要集中在与具体制造业应用的集成。

参考文献

[1] Hwang Kai, Zomaya Albert, Dongarra Jack. Distributed and Cloud Computing: From Parallel Processing to the Internet of Things[M], Morgan Kaufmann, 2010.

[2] Foster I, Zhao Y, Raicu I, et al. Cloud Computing and Grid Computing 360-Degree Compared[C]. IEEE Int. Workshop on Grid Computing Environments, pp. 1-10, 2008.

[3] SHI Chun-ming, FU Guo-kang, WEI Yi-fen. A Primary View of Desktop Cloud [OL]. [2005-01-25].http://www.ibm.com/developerworks/cn/web/1001_shimc_deskcloud/ (in Chinese)

[4] Fox A, Griffith R, Joseph AD, et al. Above the Clouds: A Berkeley View of Cloud Computing[OL]. 2009. http://www-inst.cs.berkeley.edu/~cs10/sp11/lec/20/2010Fa/2010-11-10-CS10-L20-AF-Cloud-Computing.pdf

[5] Baratto RA, Nieh J, Kim L. THINC: A remote display architecture for thin-client computing[C], ACM SIGOPS Operating Systems Review, 2005.

[6] Yang SJ. Nieh J, Selsky M, et al. (2002), The performance of remote display mechanisms for thin-client computing[C], USENIX 2002 Annual Technical Conference.

[7] Rdesktop: A Remote Desktop Protocol Client[OL]. http://www.rdesktop.org/#docs

[8] The VNC family of Remote Control Applications[OL]. http://ipinfo.info/html/vnc_remote_control.php

[9] Independent Computing Architecture[OL]. http://en.wikipedia.org/wiki/Citrix_ICA

[10] Mowshowitz A. Virtual organization[C]. Communications of the ACM, 40(9): 30-37.

[11] JING Ji-wu，LIN Jing-qiang，FENG Deng-guo：PKI Technology [M] Beijing: Science Press 2008(in Chinese)

[12] Gutmann P. PKI: It's Not Dead, Just Resting[J], Computer 35(8): 41-49.

[13] Martin F Maldonado：Virtualization Overview：View Point of Pattarn[EB/OL] http://www.ibm.com/developerworks/cn/grid/gr-virt/index.html(in Chinese)

[14] Oracle VM VirtualBox User Manual[OL]. http://www.virtualbox.org/manual/ch08.html.

[15] Rdesktop: A Remote Desktop Protocol Client[OL]. http://www.rdesktop.org/

[16] JIN Han-jun, ZHONG Hong, WANG Shuang-ding．VPN Security Practice Tutorial [M]．Beijing：Tsinghua University Press，2010:194-195(in Chinese)

[17] LI Jian-she, WU Qing-bo．VNC Safety Research and realization of VNC based on OpenSSL [J]．Microcomputer Information, 2005, 33, 6-9(in Chinese)

[18] LI Bo-hu, ZHANG Lin, WANG Shi-long et al，Cloud Manufacturing, Service Oriented Networked Manufacturing New Mode, Computer Integrated Manufacturing System, 16(1), 1-8, 2010(in Chinese)