信息中心运维实施
（堡垒机）

使用说明文档

上海体育学院

2018 年 4 月

目 录

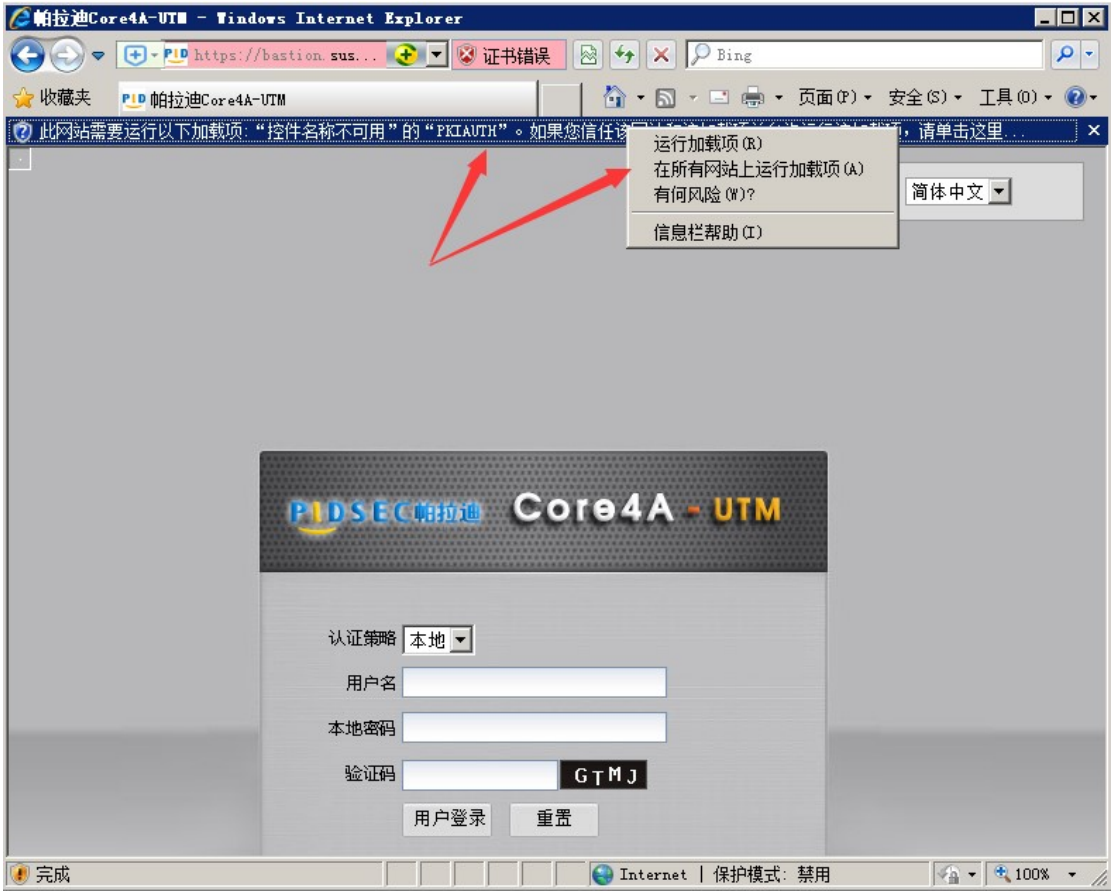
一、 实施运维的前提.....2
二、 堡垒机用户使用指南.....2
三、 堡垒机运维时可提供的资源.....5
四、 堡垒机运维的常见问题.....5
五、 实施/运维边界划分.....13

一、 实施运维的前提

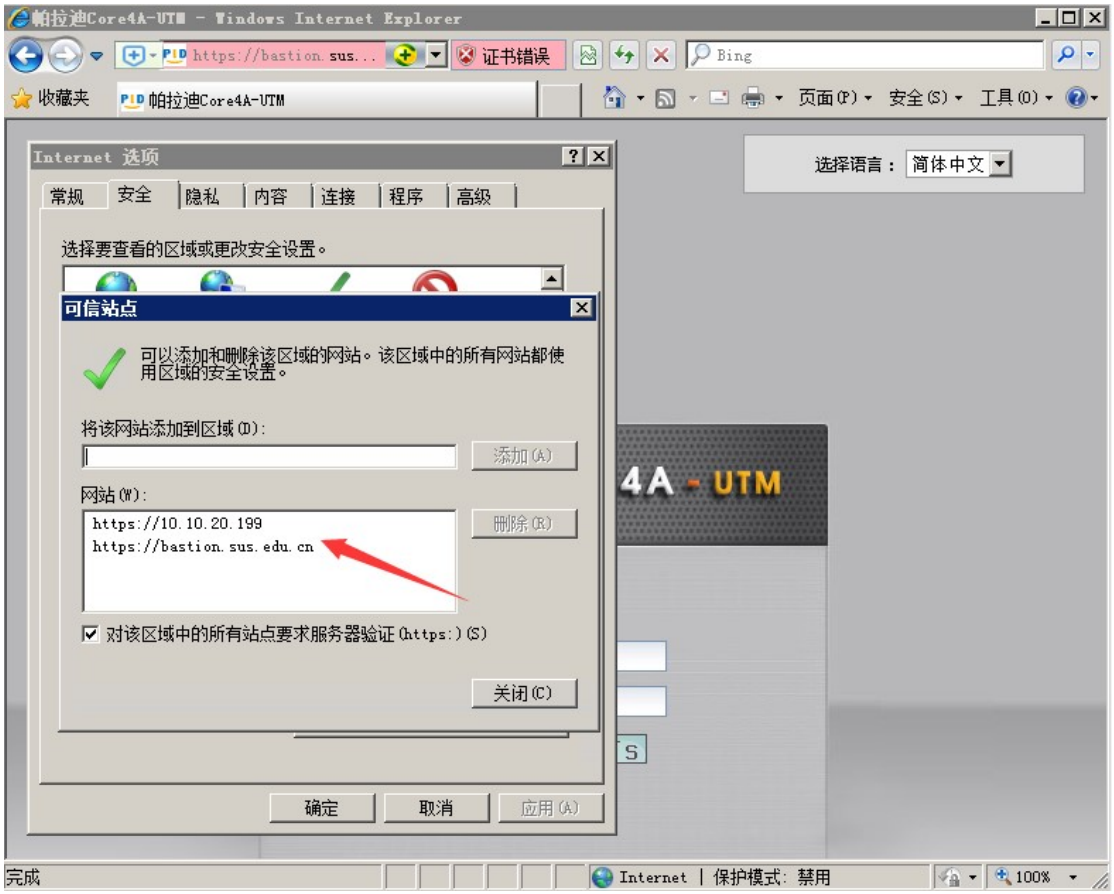
使用上海体育学院信息中心提供的运维渠道实施运维的前提要求使用者必需具备一定的 IT 技术能力，为确保能够顺利开展运维实施工作，请使用者认真阅读以下使用指南，并欢迎提出建设性意见。

二、 堡垒机用户使用指南

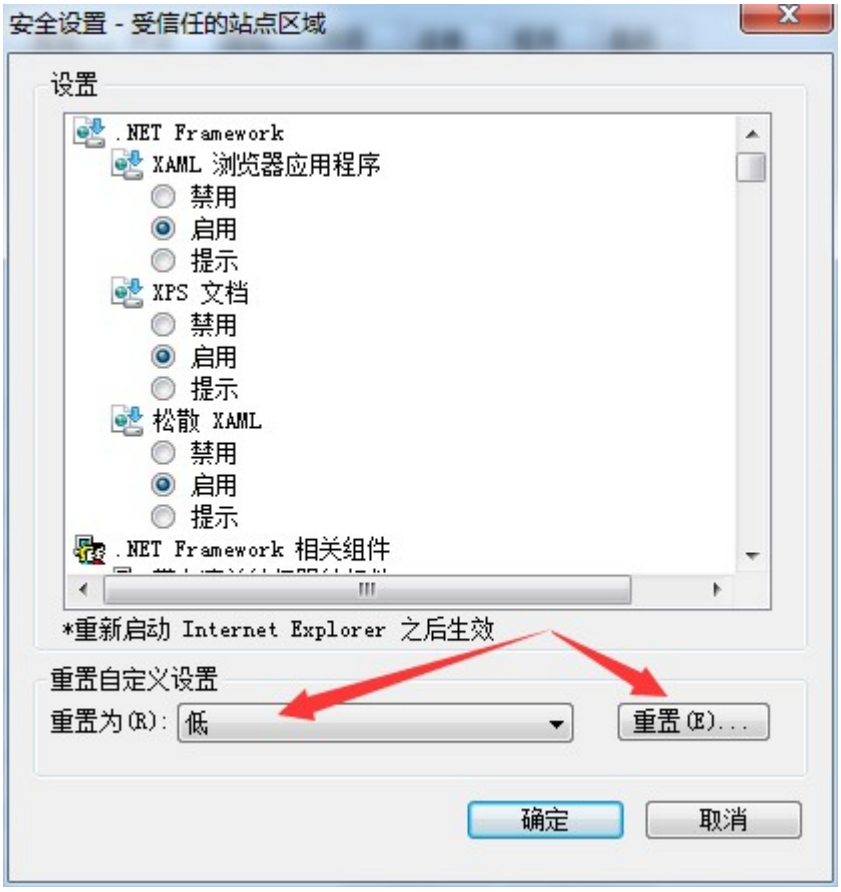
1. 互联网环境（非校园网环境）下访问堡垒机请先连接上海体育学院的 VPN，确保已经连接成功并正常登陆，使用方法参见：https://nic.sus.edu.cn/info/1018/1794.htm
2. 第一次访问堡垒机页面，建议请以管理员身份运行 IE 浏览器打开 https://10.10.20.199/或 https://bastion.sus.edu.cn/，如在地址栏下方出现加载项提示，请运行该加载项。



3. 然后打开浏览器菜单中工具/Internet 选项，选择安全标签内的可信站点，将堡垒机访问地址加入到可信站点内，随后按关闭按钮关闭窗口。



4. 同时再点击自定义级别，将安全级别临时设定为“低”，并点“重置”进行分配确定，以便第一次使用时安装堡垒机页面弹出的插件。注意，如未正常安装浏览器插件将会导致无法进行运维操作。



5. 随后可输入校方提供的堡垒机登录账号登录即可，针对具体个人账号，登录后正常情况下会强制要求修改密码后才可使用，针对公共账号则直接登录无需修改密码。修改密码规则及限制如下所示。

6. 成功登陆堡垒机后，可点击系统运维→设备组→选择授权分组→点选服务设备→运维工具，即可开始连接运维。

三、 堡垒机运维时可提供的资源

1. 堡垒机最常规的可以提供针对 Windows 环境下的非加密 RDP 远程桌面服务和 Linux 环境下的 SSH 远程连接服务。
2. 堡垒机还可提供 SFTP、Telnet、FTP、X11、PLSQL、Toad、SQLPlus、DBaccess、MySQL-Front、SQLServer、SCView4、PGAdmin、VMware vSphere Client、HTTP、HTTPS、HeidiSQL 功能，如有需要请告知学校管理者，并提供配置用的相关信息。
3. 堡垒机额外提供限制在硬件防火墙内部测试服务器环境下的 WEB 浏览测试服务，给实施或运维人员提供 IE8、IE11、FireFox、Chrome 以及 360 安全浏览器（兼容/极速）。请注意，浏览器使用 RemoteAPP 方式访问，空闲 5 分钟后断开，断开 1 分钟后该登录账号将被强制注销。

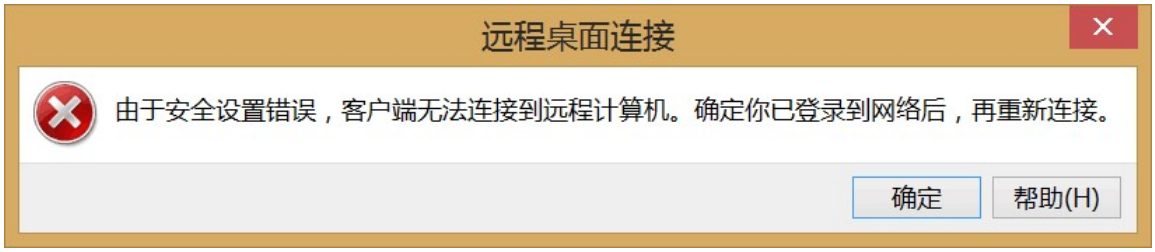
四、 堡垒机运维的常见问题

1. 已经登录了 VPN，但打不开堡垒机页面。

   处理方法：两种可能，一种是 VPN 登录不正常，可以退出 VPN 并清理浏览器缓存，再重新登录尝试。另一种是由于登录的 VPN 账号未开通访问堡垒机的权限，需要向业务对接人员沟通进行运维权限的申请，开通后方可访问。
2. 点击具体程序后提示“无法获取 Token”（如下图所示）。

处理方法：无法获取 Token 一般是由于第一次使用堡垒机时未正常安装浏览器插件所知，请使用 IE 浏览器并将将浏览器的自定义级别降到最低并重置设置后，再刷新访问一下一般可以正常使用了，退出注销堡垒机账号后建议恢复自定义级别设置。

3. 使用的 Win8/Win10 在打开远程桌面时提示“由于安全设置错误，客户端无法连接到远程计算机。确定你已登录到网络后，再重新连接。”（如下图所示）



处理方法：打开"本地安全策略"- Win+R 并输入 secpol.msc（或者在"管理工具"中打开）。在本地安全策略中，打开“本地策略”下的“安全选项”。在右边的策略中，找到“系统加密：将 FIPS 算法用于加密 、哈希和签名”点击右键属性。将“本地安全设置”设置为“已禁用”，在单击“应用”，后“确定”，即可远程控制！

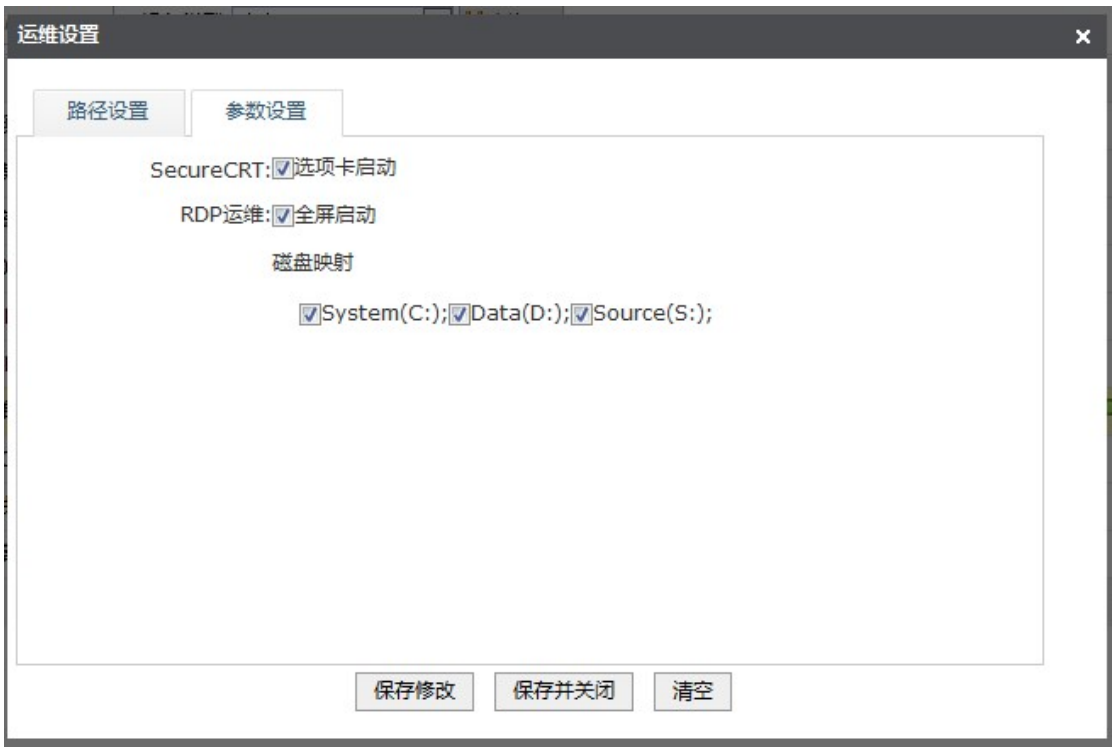
4. 打开具体程序时提示“Please set the program path”（如下图所示）。

处理方法：该问题是由于没有配置打开程序的有效路径所知，前提是本地已经安装过了该程序，然后打开页面右上角的运维设置，在弹出界面中的路径

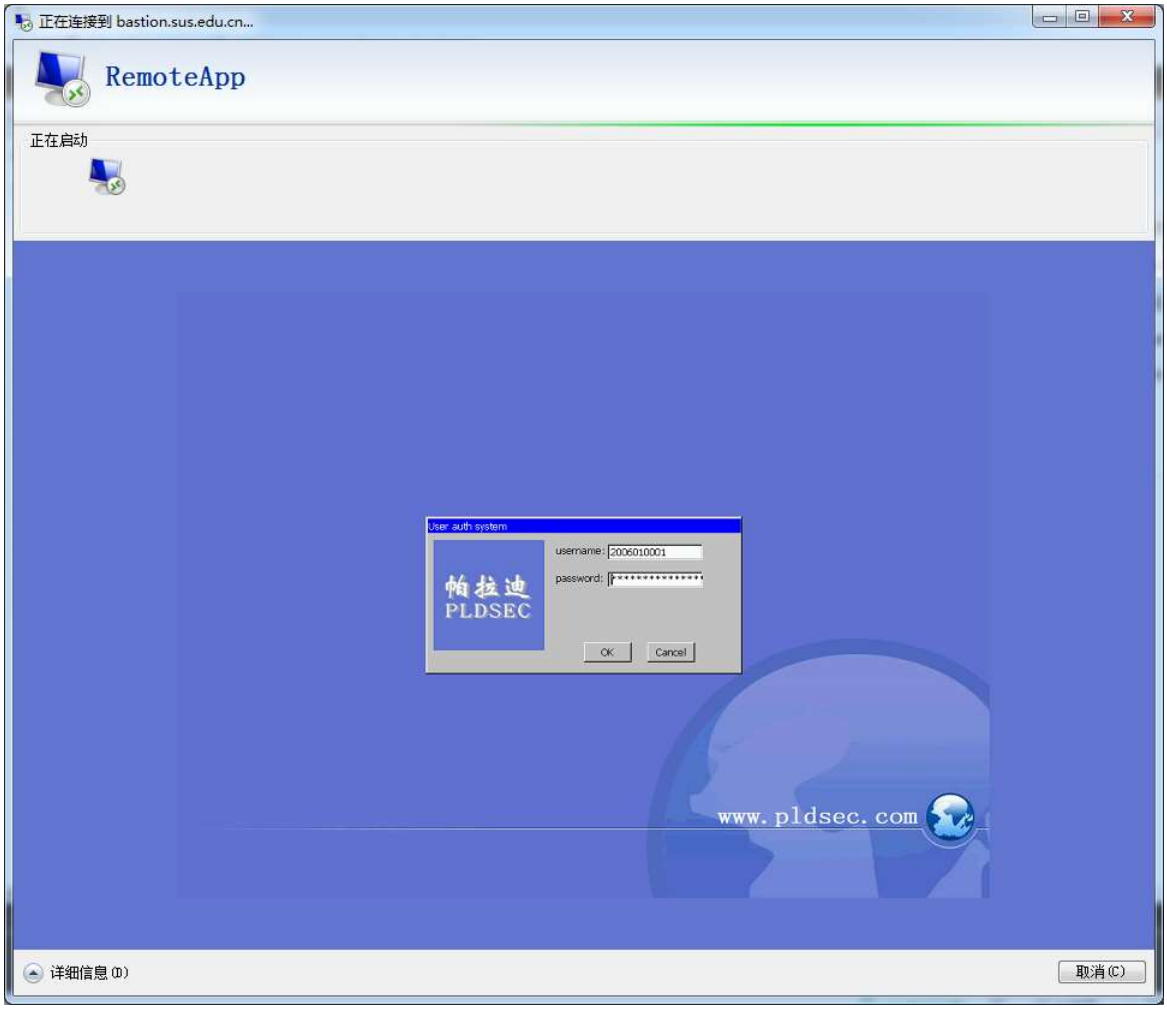
设置界面内（如下图所示）。将相应程序在本地安装的实际文件名路径输入到对应名称后方的框内，最后保存关闭，即可访问。

5. 需要调取本地计算机内磁盘中的内容，或者需要将远端内容保存本地计算机磁盘内，但实际操作中看不到本地磁盘？

处理方法：该问题需要堡垒机管理员和实施或运维人员两侧均进行配置才能实现。首先实施与运维申请时要向业务对接人员告知开通映射本地磁盘的权限，在堡垒机管理员审核后方可开通。其次在操作实施、运维的终端上登录堡垒机界面，在右上角的“运维设置”/“参数设置”中勾选“RDP 运维”的“磁盘映射”内具体盘符后保存（如下图所示）。最后在打开应用连接时下拉详细信息，勾选好驱动器后，才能实现磁盘映射的功能性操作。



6. 有时候打开应用的时候会卡在用户登录界面不会继续（如下图所示）？



处理方法：该问题厂家答复为有时候由于网络问题出现这个蓝色登录界面，关闭下重新再点击打开就可以使用了。第二种情况是由于堡垒机登录超时了，也会出现该问题，此时需要重新登录堡垒机后才能继续正常使用。第三种情况一般是由于网络不稳定所导致的，可以通过重连 VPN 及堡垒机后再次尝试。

7. 需要在堡垒机分配的应用里实现与本地的复制粘贴功能。

处理方法：该问题需要堡垒机管理员和实施或运维人员两侧均进行配置才能实现。首先实施与运维申请时要向业务对接人员告知开通与本地交互复制粘贴的权限，在堡垒机管理员审核后方可开通。然后在操作实施、运维的终端上登录堡垒机，在打开应用连接时下拉详细信息，勾选好剪贴板后，就能实现与本地的复制粘贴的功能性操作（如下图所示）。

8. 除了 RDP 远程桌面和 SSH 连接，其它应用有时候打不开，或者打开后自动跳掉？

   处理方法：除了微软 RDP

和 SSH 基本可以正常打开外，其余非堡垒机内置工具是利用 RemoteApp 发布出来应用程序，此时点击非红 R 的图标后会出现打开（登录）后自动跳掉（注销），遇到这种状况，尽可能使用有带红 R 字样的图标方式打开，如 等，如出现长时间正在加载的情况，可下拉详细信息来观察打开处于哪个阶段或者碰到需要交互式问题，并可向信息中心反应。

9. 堡垒机默认用 WinSCP 打开系统的 SFTP 只能看到 root*****目录，无法看到根目录？

   处理方法：堡垒机的安全策略授权仅允许登录到登录用户账号的 Home 目录，不能直接访问根路径，操作人员可以以此为跳转，先传输到用户的 Home 目录，然后再将文件转移到具体位置中去。

10. 堡垒机在登录时确定登录账号是正确的，但等待图标一直在滚动且无响应，一段时间后仍然反馈登录账号存在问题无法进入系统。

    处理方法：此为已知可能存在的问题，如登录时遇到此问题请及时通过信息

中心进行处理。

11. 堡垒机登录时处于英文状态，如何修改成中文？

处理方法：请在堡垒机登录界面右上角点击 Language 处下拉菜单，可有 English 英文和 Chinese Simplified 简体中文给予选择。

12. 堡垒机登录时提示“您的密码已经过期!”，但又没有修改密码的地方？

处理方法：此问题是由于堡垒机的密码策略限制所引起，请知晓，密码有效期为 42 天，系统将会提前 10 天给予用于提醒，同时会在密码过期后 100 天内允许用户自行修改密码，如果超过了 100 天就会出现如下图所示告知密码已经过期，但也已经不允许用户自行修改的权限了。

13. 堡垒机打开应用时提示对话框“Token error”，无法使用程序？

处理方法：从现象描述应该是无法调取堡垒机的插件所致。目前已知的一种情况为有其他版本的同名插件文件影响了该版本的堡垒机插件的正常调用，包括已知的 x:\Windows\SysWOW64\ 文件夹下的 termappcall.dll / pkiauth.dll / pldota.dll 等，解决途径是删除这些文件，然后重新打开浏览器加载一下堡垒机插件即可。

14. 在使用堡垒机提供的 WEB 浏览器时，会出现点击后自动跳掉，或者一直打不开状态？

处理方法：自动跳掉请参考常见问题第 8 条进行处理。如遇见浏览器一直打不开情况，则有另一种情况，是由于该浏览器对于多用户并发支持兼容性存在问题，此时此刻已有其他用户先于你打开了该浏览器，导致后续用户无法正常使用，遇到该情况可以稍后再试，等到已在用的用户用完且账号注销后，方可正常使用。

我们经过多次测试，现内部浏览器中 Google Chrome、360chrome、360se 存在多用户不太兼容的情况，Internet Explorer 11、Microsoft Edge 和 Mozilla Firefox 对多用户使用兼容性良好。

15. 通过堡垒机的 sftp 传输文件非常慢，甚至只有几 k/s？

处理方法：已知 sftp 复制非常的原因有两种，一是传输的文件又散又多，会出现像 windows 中复制散文件一样的慢速情况，1 千万个 1k 大小的文件传输速度肯定要比 1 个 10G 大小的文件慢上许多的原因是一样的，因此建议先打 zip 包形成一个单独文件后传输至服务器，再在服务器上解包后使用。二是网络带宽受限或不稳定导致，学校接入默认是中国电信宽带接入，异架构宽带或北方/国外带宽可能会导致传输慢，此类问题暂无根治方案，可联系信息办项目对接人，通过实施通讯工具（如 QQ，微信等）暂传到校内信息办对接人处后，再由对接人代为上传至服务器。

五、 实施/运维边界划分

信息系统项目建设时信息中心与项目系统部署实施/运维团队的责任边界划分为：

信息中心：负责数据中心提供项目系统的机房环境、服务计算资源、操作系统初始交付、公共数据库环境、堡垒机。

项目系统部署实施/运维团队：负责操作系统、独立建在操作系统上层的中间件（IIS、Apache、Nginx、Tomcat、PHP、Java 等）、独立数据库、程序代码、提

供的接口。

共同负责：程序对接、集成的内容。