linux认证:SAMBA连接过程中的常见错误解析Linux认证考试
PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/580/2021_2022_linux_E8_AE_A4_E8_AF_c103_580585.htm 通过SAMBA可以让Linux服务器成为Windows域中的一员，也可以让Windows客户端通过网上邻居来访问Linux服务器。不过Windows与Linux毕竟是两个不同的操作系统平台。即使SAMBA服务器提供了双方沟通的一个平台，但是在联机过程中仍然会出现一些问题。我今天就这些常见的问题进行一些说明，并提供一些解决措施。希望这些内容可以帮助系统管理员解决日常工作中遇到的难题。一、XP客户端可以登录，2000客户端却不可以。 刚开始采用SAMBA服务器的时候，遇到过一个奇怪的问题。那时企业中客户端还没有完全统一，主要有2000客户端与XP客户端。在部署 SAMBA应用的时候，却发现一个奇怪的问题，只有XP客户端可以通过网络邻居来访问Linux服务器.而其他客户段却不行。经过一系列的措施后，我终于发现了问题所在。 这主要是Windows操作系统与Linux操作系统在密码的处理机制上不同。目前主流的Windows操作系统都已经使用加密的方式来发送密码。而在SAMBA服务器上，则系统管理员可以决定是否要指定用户密码必须以加密的形式发送到SAMBA服务器，利用encrypt passwords选项来确定。如果这个选项设置为NO，则所有的Windows客户端都将不能够登陆到Linux服务器上。为此，笔者把这个选项设置为 YES后，即指定用户密码必须以加密的形态发送到SAMBA服务器。然后所有的Windows客户端就都可以正常登陆到了Linux系统服务器了。 那么为什么以前只有XP客户端可以登陆，而2000客户端不

能够登陆了?查找了相关的资料并经过测试后，发现如果把以上这个选项设置为NO的话，则必须要通过修改客户端的配置来实现。如需要把SAMBA服务器软件包中的一个文件复制到客户端上。只有如此，在没有启用encrypt passwords的基础上，Windows客户端才可以正常连接到Linux服务器上。 如上图所示，在SAMBA安装目录下有Registry这个文件夹。这个文件加中存储着一些密码处理文件。如果把选项encrypt passwords设置为NO的情况下，则需要把这些文件复制到对应的Windows客户端下，否则的话就不能够正常登陆。笔者把Win2000这个注册表文件复制到2000客户端，并双击直接把注册表的值倒入到注册表中。重新启动客户端后，2000系统就可以顺利访问Linux服务器了。 为此我觉得大部分情况下还是把encrypt passwords选项设置为YES好。如果有特殊的需要(如出于访问控制的需要等原因)，则可以把这个选项设置为No。然后把这些注册表文件复制到对应的客户端上，以保证需要访问的客户段可以正常连接到Linux服务器上。 二、不支持大写密码。 为了保障Linux服务器上资源的安全性，为连接设置密码是必须的。但是我在部署SAMBA服务器过程中，却发现一个非常奇怪的问题。原来在为SAMBA服务器设置访问密码的时候，竟然不支持全部为大写的密码。也就是说，密码若全部为大写ABCDEF则Linux服务器不认可.但是abcdef则是认可的。这到底是什么原因呢? 在Windows操作系统中，虽然对于密码的大小写是敏感的，但是对于密码中大写字符的个数则没有限制。但是SAMBA服务器则不同。在SAMBA服务器中，有一个参数password level。大家不要误解以为这是一个设置密码安全等级的选项，其实不是。这个选项主要用来

设置SAMBA服务器允许的大写密码的字符数。如把这个参数设置为3的话，则在密码设置中只允许三个大写字符。如果密码为六为，全部为大写字符的话，则SAMBA服务器就不会接受这个密码。显然这是一个比较糟糕的设计。因为在Windows客户端中没有这个限制，而在 SAMBA服务器有这个限制，则容易造成他们之间的不兼容。如果企业用户喜欢利用大写字符作为密码的话，则需要更改这个参数。如系统管理员规定密码的最大长度为8位，则就需要把这个选项的值设置为8。 三、某些IP地址的客户端无法正常访问。 有时候企业的客户或者供应商到企业进行访问的时候，也需要用到企业的网络。他们会有自己的笔记本电脑，然后通过企业的网络进行互联网访问或者与其它员工进行文件交换等等等。为了Linux服务器上资源的安全，我就在服务器上设置只有企业的客户端电脑可以访问Linux服务器。这个设置也比较简单，只要通过IP地址来限制即可。如在SAMBA服务器下，有一个/etc/samba/smb.conf的配置文件。在这个文件中，有一个hosts allow的参数，就可以用来设置允许访问的客户端。 默认情况下，这个参数是不起作用的。也就是说，所有的客户端只要有合法的用户名与密码都可以正常访问Linux服务器。但是如果在这里进行限制的话，则首先需要IP地址合法，服务器才会进行密码与用户名的校对。如果IP地址都不合法的话，则即使有合法的用户名与密码，也无法正常访问Linux服务器。如果要启用这项功能，可以把这个参数前面的注释符号去掉。注意在这个配置文件中，注释符号是冒号(：)。而不是Linux系统配置文件中的#号。这个细小的差异各位系统管理员需要注意。 所以到企业中的客户端，有几台客户端不

能够正常通过SAMBA服务器访问Linux操作系统上的共享资源，而其他客户端可以正常访问的话，则需要系统管理员就需要考虑是否是这个参数在作怪。最简单的测试方法就是先把这个参数禁用掉，然后再测试一下客户端看能否正常连接到Linux服务器上。如果可以连接了，则说明是这个参数配置有错误。此时系统管理员就需要仔细检查这个参数的配置，看看有没有把这些客户端的IP地址加入到这个参数列表中。如果禁用掉这个参数之后还不启作用的话，则可能是其他方面的原因了。不过通常情况下，都是因为这个参数中的IP地址配置不当所引起的。 顺便说一句，通过IP地址来限制客户端连接到SAMBA服务器的话，并不是很安全的处理措施。因为服务器无法控制客户端上IP地址的更改。如果一定要采用这种方式的话，则需要其他设备的帮助。如可以在路由器上实现IP地址与MAC地址的帮定，让客户端无法更改IP地址。从而提高这个安全机制的安全性。 四、日志文件太过于庞大。 在SAMBA服务器中，也有日志管理的功能。即企业用户通过SAMBA客户端登陆到Linux服务器后所有的操作都会在日志中留存相关的记录。这主要是为了方便后续的维护以及安全方面的需要。但是有时候日志文件管理不当这也会成为一种负担。如一年以来的日志信息都保存在同一个文件中，那么这个文件就会变得非常的庞大。管理员光打开这个文件可能都需要一定的时间.而去查找相关的内容则可能需要花费更多的时间。而且这个日志文件日益庞大，也会对服务器的硬盘空间产生比较大的压力，会影响Linux服务器的性能。 为了解决问题，在SAMBA的全局配置文件中提供了一个max log size的参数。默认情况下，这个参数的值为0，即对于日志文件没

有大小的限制。系统管理员可以企业的实际情况来设置这参数。如可以把这个参数的值设置为 200KB(这个参数的单位为kb)。服务器会定期检查这个上限值。如果超过这个设置的话，系统会关闭这个日志文件并重新命名这个日志文件，并会在日志文件名字中加入old.然后重新建立一个日志文件。注意，这里并不是把原先的日志文件覆盖掉，而只是把新的日志信息保存到一个新的日志文件中，即进行分文件处理。为此系统管理员仍然需要根据硬盘的大小来手工清理一些过期的日志文件信息。为了防止日志文件过大过多对Linux服务器性能的影响，我建议各位系统管理员，最好能够把这个日志文件定位到一个独立的硬盘或者分区文件中。如可以用过log file参数来重新制定日志文件的存储路径。 