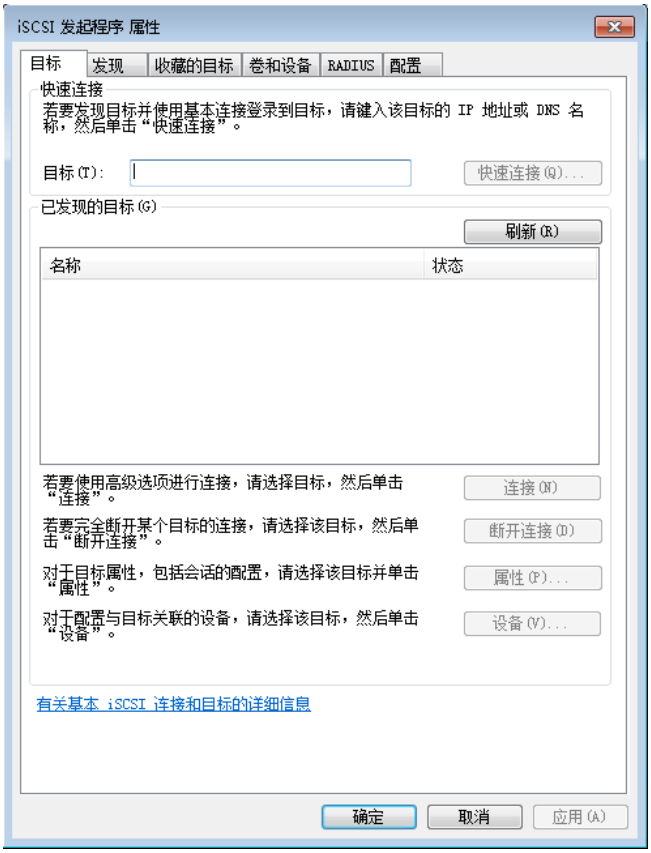
Windows通过iSCSI挂载P5730存储卷失败问题排查经验案例

主机相关 存储配置 黄磊 2018-03-19 发表

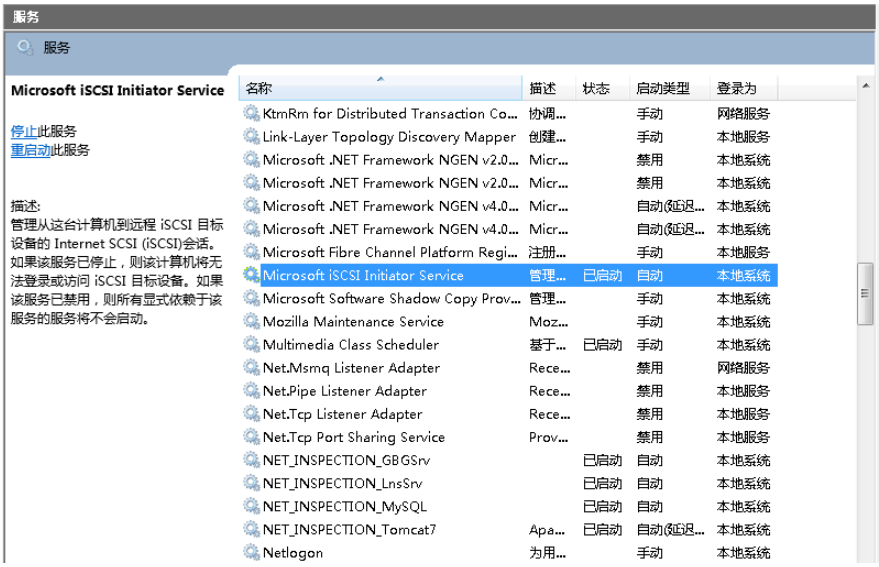
H3C FlexStorage P5000存储是一款横向扩展存储平台，专为满足虚拟化环境不断变化的需求而设计。支持iSCSI（Internet Small Computer System Interface 互联网小型计算机系统接口）存储协议，能够在IP协议上层运行SCSI指令，从而使网络上的主机系统（Initiator端）通过IP网络就能够访问到存储资源（Target端）。在遇到Windows系统主机挂载FlexStorage P5730存储卷失败时，可以参考本案例完成初步的问题定位。

1、iSCSI发起程序

iSCSI发起程序是Windows系统下的一款连接iSCIS Target也就是iSCSI存储的客户端软件，现在已经内置于如Windows 2008等系统中，如下图。如果没有请先正确安装iSCSI发起程序。

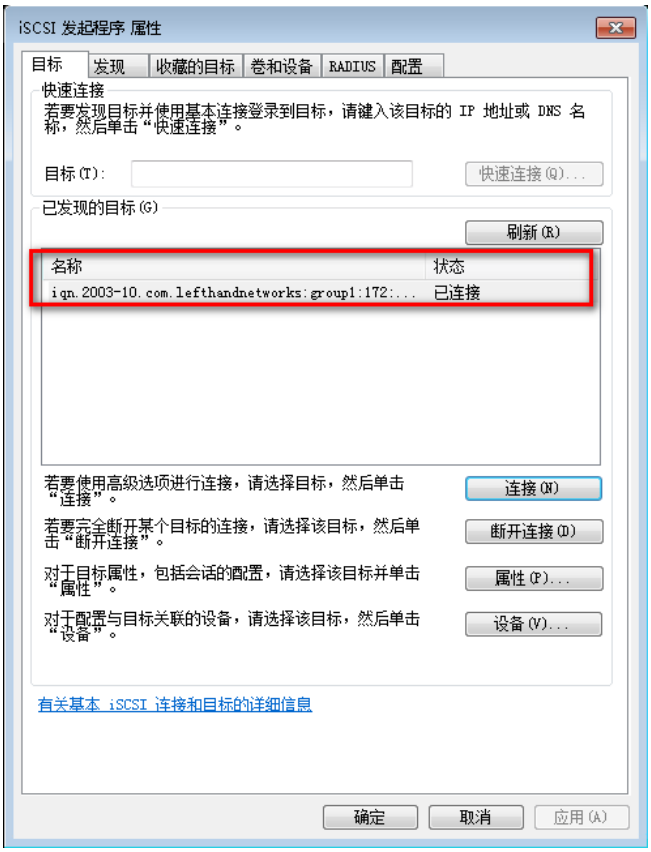


iSCSI发起程序的运行还需要依赖“Microsoft iSCSI Initiator Service”服务，正确安装iSCSI发起程序后，并检查该服务是否正常启动，如果没有启动，请在Windows“服务”中启动该服务。

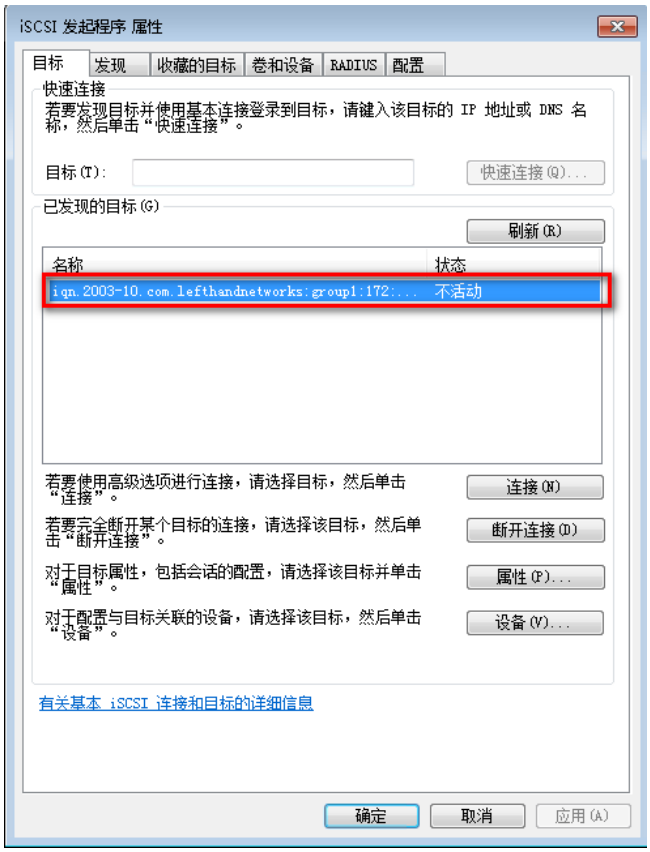


2、是否发现Target

Windows已发现的存储Target会显示在iSCSI发起程序的“目标”菜单中，已正常挂载的存储Target状态显示为“已连接”。



已发现的Target状态显示为“不活动”时，请选中对应的Target后点击“连接”按钮。

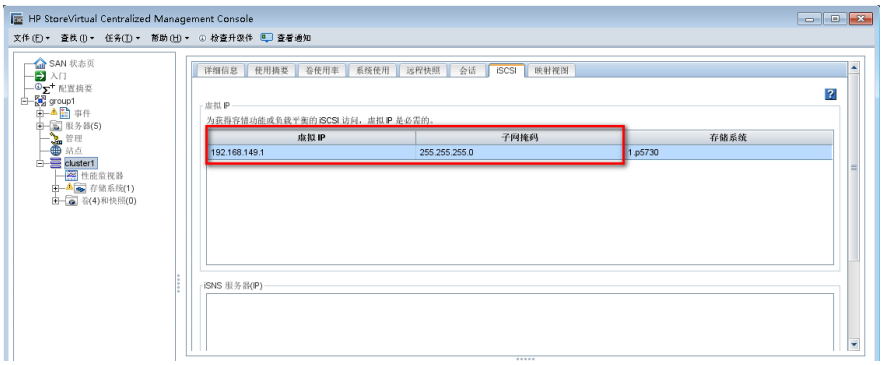


推荐勾选“将此链接添加到收藏目标列表”，便于以后系统启动时自动连接Target。

3、网络是否可达

由于iSCSI协议承载在IP上层，使用TCP 3260端口，需要确保主机系统到存储提供业务的虚拟IP地址之间网络可达。可以通过ping等工具测试网络连通性。

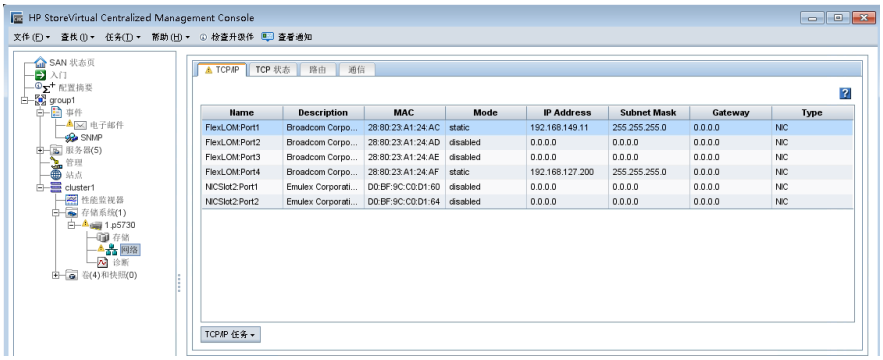
存储的虚拟IP地址可以通过CMC（Centralized Management Console）登陆存储管理组，选中对应的集群后，点击“iSCSI”后查看，如下图。



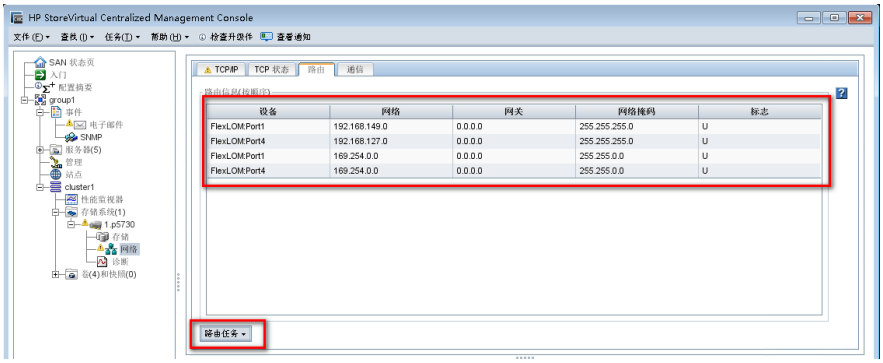
4、排查网络问题

检查网络配置主要包括：

1） 检查存储虚拟IP地址和承载业务的网卡IP地址为同网段。存储节点网卡地址可以在存储节点“网络”中的“TCP/IP”菜单下查看。



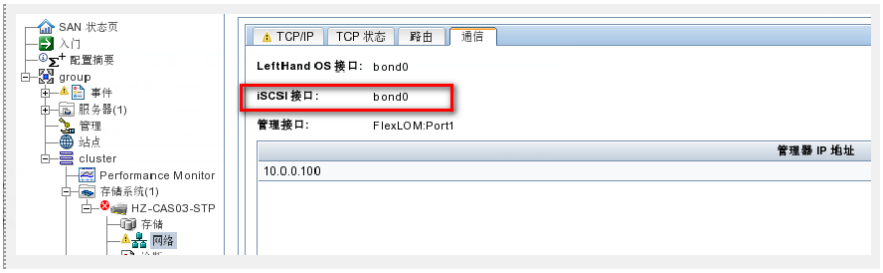
2） 检查是否有到主机系统地址的路由信息，并且“设备”为业务网卡。如果路由信息不正确，可以点击“路由任务”编辑路由信息。



3） 检查主机系统到存储之间的网络设备配置，如果有经过安全设备，确保安全策略中放行存储虚拟IP地址的TCP 3260端口。

5、检查iSCSI接口

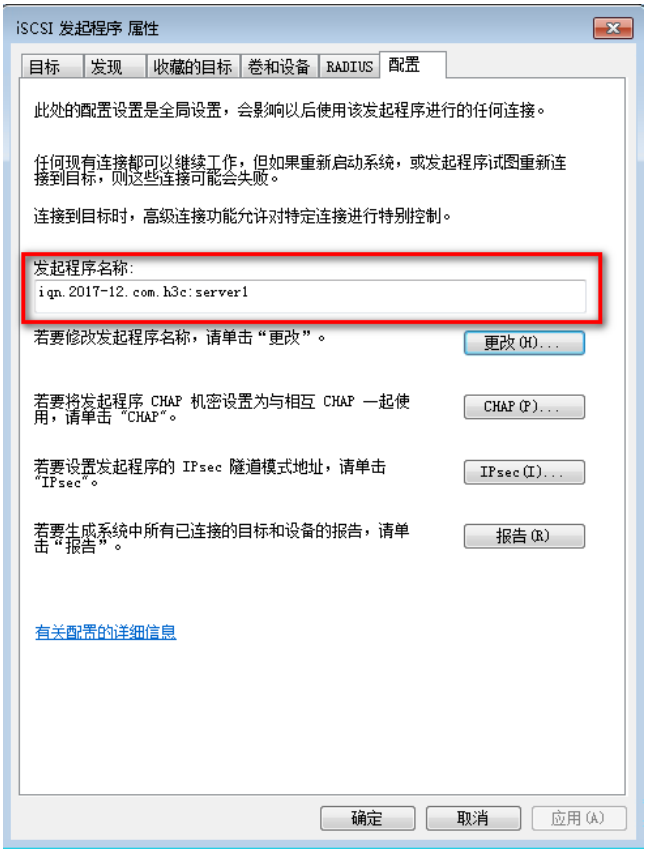
H3C FlexStorage P5000存储上有不同的接口角色定义，其中iSCSI接口定义为对外提供iSCSI连接服务的接口角色，需要将对外提供业务网卡配置成iSCSI接口后，存储通过虚拟IP地址才能提供iSCSI连接服务。



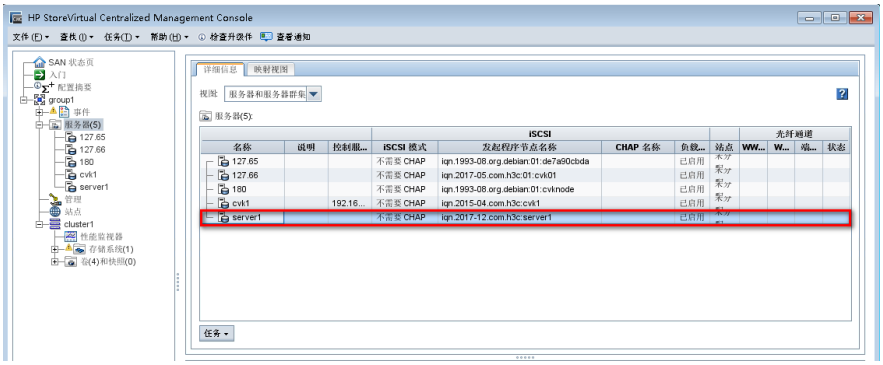
6、iSCSI Name配置

iSCSI的识别机制是基于名字的，这个名字一般被称为iSCSI Name。建立连接时，Initiator端发起一个连接请求，Target端收到请求后，确认Initiator端发起的请求中所携带的iSCSI Name是否与Target端绑

定的iSCSI Name一致。如果一致才能建立iSCSI通信连接。iqn规范定义的发起程序名称格式为“iqn.domaindate. reverse.domain.name:optional name”，例如：iqn.2017-12.com.h3c:server1。
在iSCSI发起程序的“配置”菜单中检查发起程序名称配置是否规范。



通过CMC登陆存储管理组后，选择“服务器”，对应服务器配置中的“发起程序节点名称”和主机系统iSCSI发起程序中配置的“发起程序名称”需要完全一致。



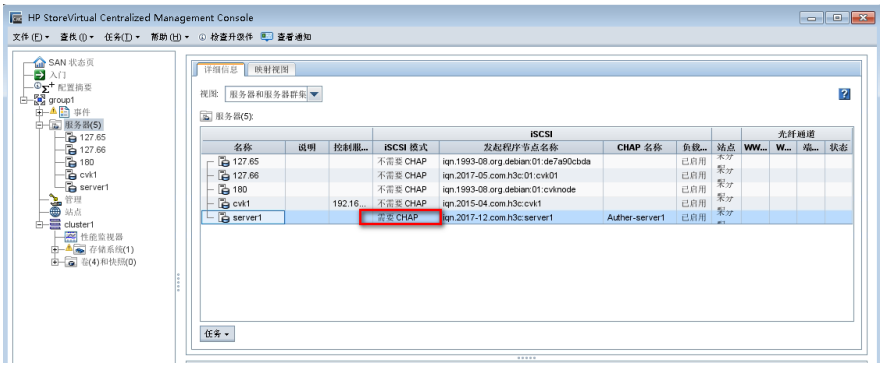
如果不一致，请编辑服务器在“发起程序节点名称”处更改。

7、是否启用认证

iSCSI可选配CHAP认证，细分为Initiator认证和Target认证。Initiator 认证要求在Initiator尝试连接到一个Target的时候，Initator需要提供一个密钥给Target供Target进行认证。Target 认证要求在Initiator尝试连接到一个Target的时候，Target需要提供一个密钥给Initiator供Initiator进行认证。

Initiator认证可以在没有Target 认证的时候应用，这种只要求Target验证Initiator的CHAP认证也称为单向认证；Target认证则要求Initiator认证被同时应用才可以，也就是说，Initiator和Target需要相互认证，这种认证被称为相互认证。

存储上是否配置启用认证可以在CMC的“服务器”配置菜单中查看“iSCSI模式”确认。



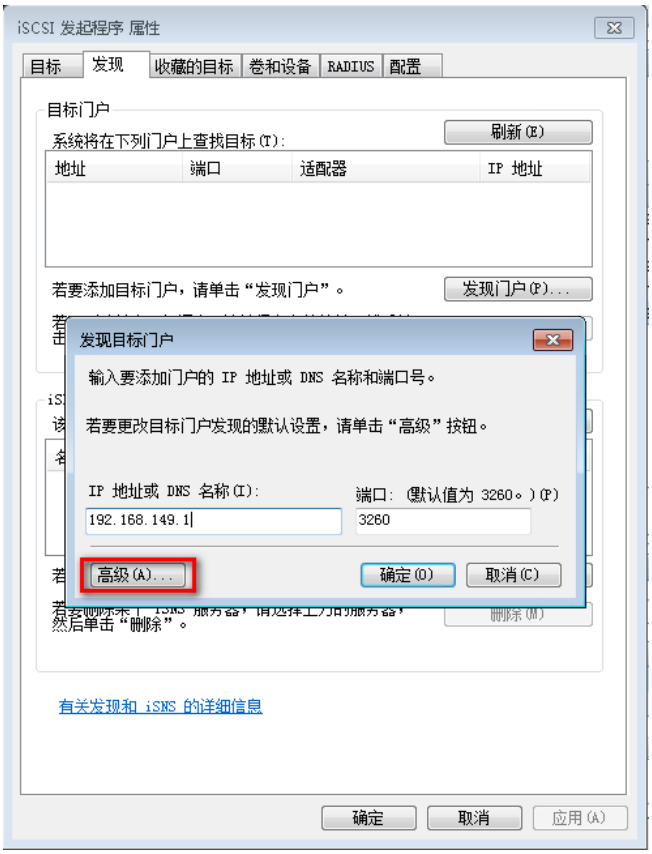
8、认证方式和密钥

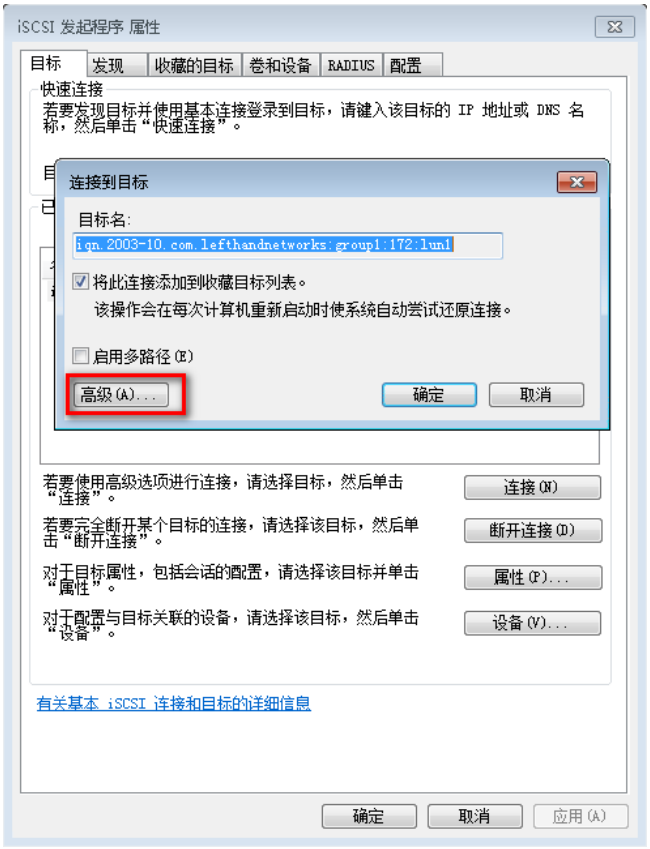
如果启用CHAP认证，需要在存储设备侧和主机系统侧检查是配置单向认证还是双向认证，并且两端对应的认证密钥需要一致。 CHAP认证密钥长度要求必须长于12位。

1） 单向认证

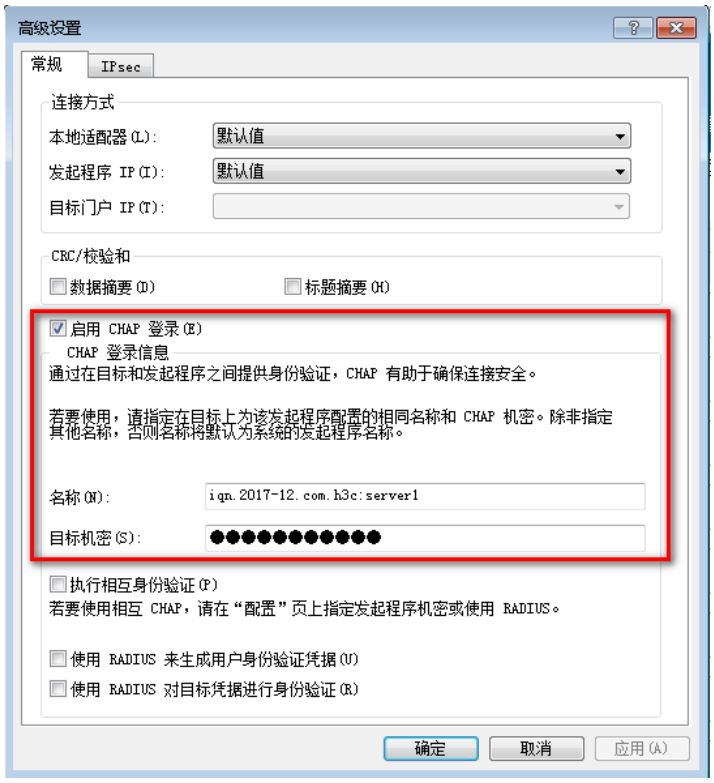
存储设备侧CHAP认证在新建或者编辑服务器菜单中配置，如下图，配置。单向认证需要配置“目标机密”。

主机系统侧，需要在iSCSI发起程序中添加目标门户和连到接到目标时，进入“高级”选项下配置。





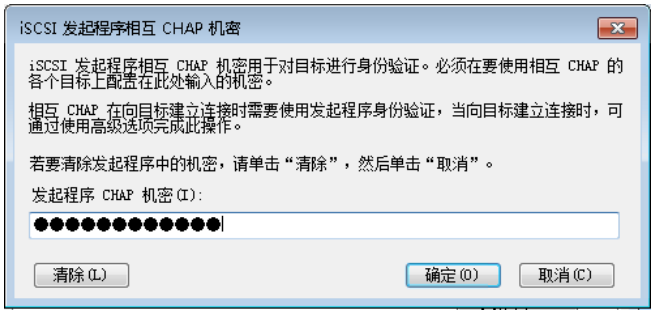
勾选“启用CHAP登陆”，配置“目标机密”，和存储设备侧密钥配置一致。



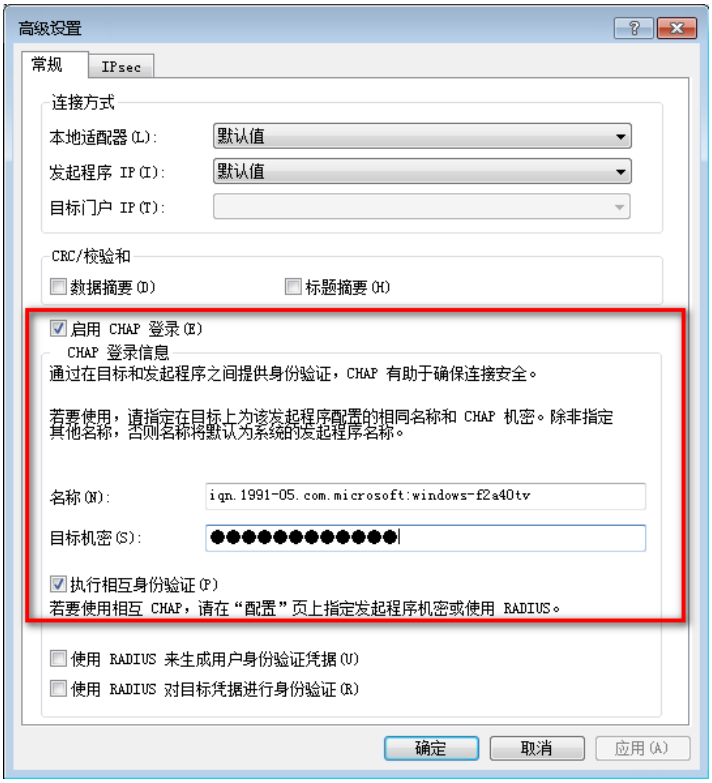
2） 双向认证

存储设备侧在新建或者编辑服务器菜单中配置“目标机密”和“发起程序机密”。

主机系统侧“发起程序机密”在iSCSI发起程序的“配置”菜单中点“CHAP”按钮后配置。



“目标机密”需要在iSCSI发起程序中添加目标门户和连到接到目标时，进入“高级”选项下配置，除了勾选“启用CHAP登陆”、配置“目标机密”外，还需要勾选“执行相互身份验证”。



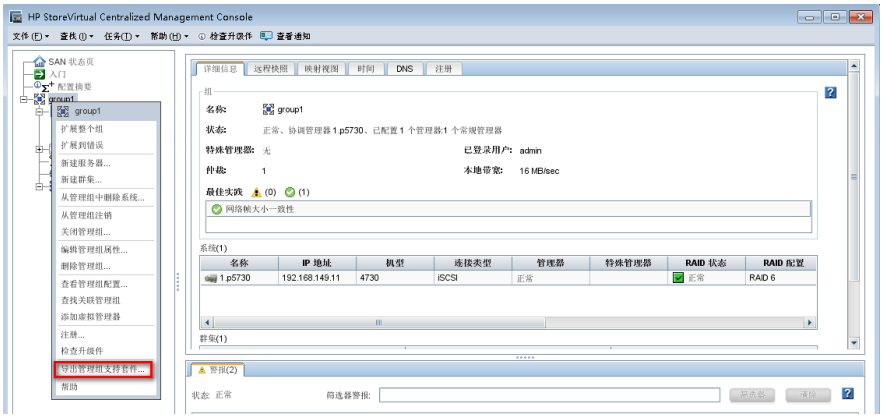
9、集群和卷配置

检查存储集群下正确配置存储卷，并且存储卷分配给服务器。

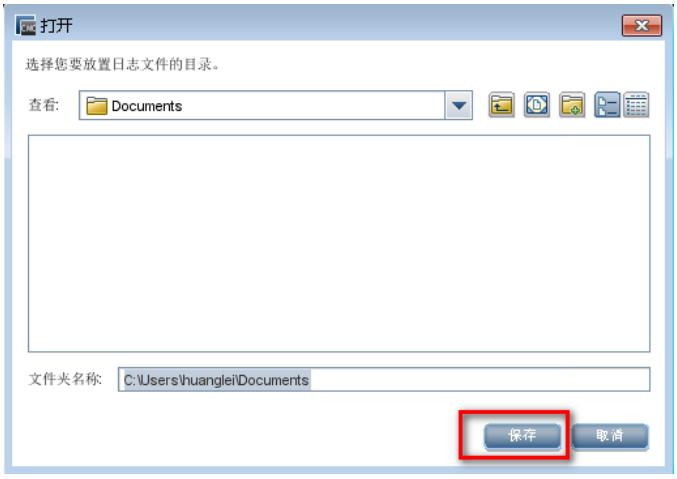
如果安装以上步骤依旧无法解决，那么建议通过CMC登陆存储管理组后，查看管理组状态和事件告警、收集存储管理组支持套件和存储iLO AHS日志、操作过程相关截图，联系H3C技术支持热线 400-810-0504进行分析。下面介绍存储管理组支持套件和存储iLO AHS日志收集方法：

1） 存储管理组支持套件信息收集

通过CMC连接存储管理组后，选中管理组右击，选择“导出管理组支持套件”选项。



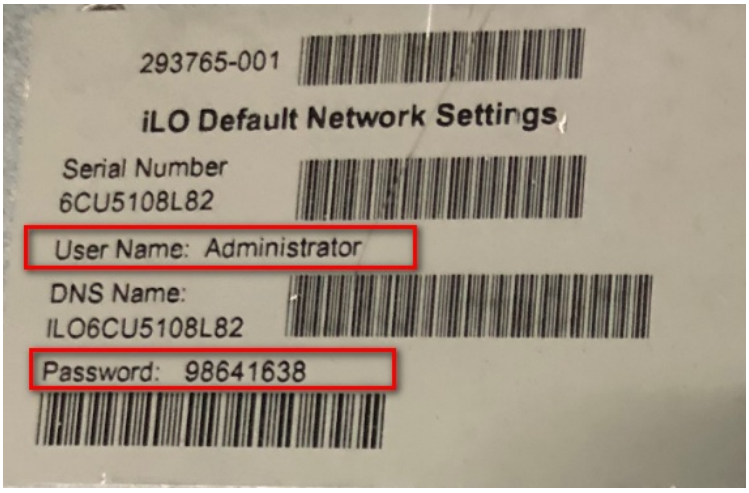
选择存储管理组支持套件信息保存的路径后点击“保存”按钮。



存储管理组支持套件文件生成生成后，在对应的文件夹中能查看到对应的.zip文件。

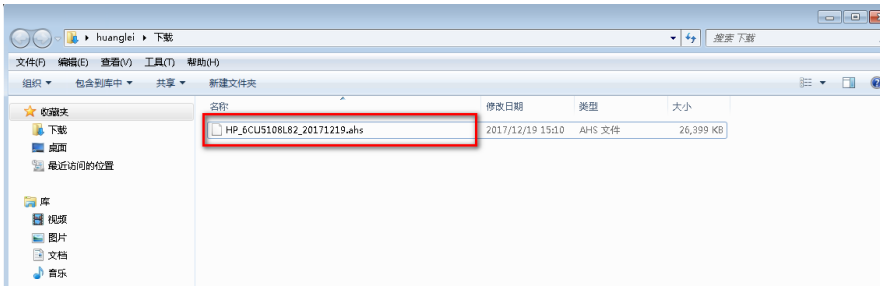
2） AHS日志收集

通过WEB方式开的iLO管理界面，输入账号登陆。iLO配置了缺省用户名和密码，缺省用户信息可以在存储设备左上角的贴牌上查看。



WEB正常登陆后，在“信息>Active Health System日志”菜单下，设置好收集日志的时间范围，点击“下载”。

推荐使用IE浏览器操作，生成的日志文件后缀名以.ahs结尾。


huanglei ▸ 下载
搜索 下载
文件(F) 编辑(E) 查看(V) 工具(T) 帮助(H)
组织
包含到库中
共享
新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
名称
修改日期
类型
大小
HP_6CU5108L82_20171219.ahs
2017/12/19 15:10
AHS 文件
26,399 KB