UNIS A2000-E运维管理系统

故障排查手册

关于本文档

本文档介绍了用户在使用A2000-E 运维管理系统过程中的故障处理方法。

格式约定

格式	说明
粗体	各类界面控件名称采用**加粗**字体表示，如单击**确定**。
>	多级菜单用 **>** 隔开。如选择**用户管理** > **用户列表**，表示选择**用户管理**菜单下的**用户列表**子菜单。

目录

通用故障排查方法

1

目录:

一般流程

故障排查的通用流程如表 1: 故障处理一般流程所示。

表 1: 故障处理一般流程

步骤	动作	动作说明
第一步	了解问题	明确问题的现象、复现频率、复现方法、环境和影响。 对于问题现象，需要明确预期和实际结果、如果有错误提示需要记录错误提示。
第二步	确认问题	确认问题是否是配置问题、是否产品的问题、是否是已知问题。对于配置问题可以参考产品相关的用户手册查询正确的配置。如果不是产品的问题，需要明确导致问题的外部组件。如果是已知问题，可以尝试升级解决，或者等待补丁发布。
第三步	排查问题	在确认问题后，可以参考本手册中相关的业务模块排查问题。
第四步	收集信息	如果参考本手册中的故障排查思路依然无法解决问题时，请收集问题相关的信息，具体包括: • 问题描述 • 复现频率 • 复现方法 • 影响 • 环境 • 你的排查过程和结果 • 日志，关于日志收集请参考收集日志
第五步	反馈问题	向您的技术接口人反馈问题，寻求进一步的技术支持。

常用方法论

对于陌生的异常问题，很多人会感到无从下手，不知道从哪里开始。此时如果掌握一些基本的排错方法论就可以避免这种无力感。对于新手方法论可以告诉你从什么地方开始，并列举了如何继续下去的步骤。对于专家，方法论可以作为检查清单来使用，确保没有遗漏。《性能之巅》中介绍了很多性能调优的方法论，同样适合故障排查，我们节选部分，有兴趣的可以阅读原文。

问题陈述法

明确问题如何陈述是技术支持人员开始反映问题时的例行工作。通过询问客户以下问题来完成：

1. 是什么让你认为存在问题?
2. 系统之前运行得好吗?
3. 最近有什么改动？配置？网络？客户端？并发?
4. 问题有什么影响？会影响普通用户么?
5. 环境是什么样的？客户端操作系统版本？浏览器版本？我们的软件版本？有特殊的配置么？目标设备是什么版本?

询问这些问题并得到相应的回答通常会立即指向一个问题和解决方案。当你遇到一个新问题时，首先应该使用的就是这个方法。

Ad Hoc核对清单法

当需要检查和调试系统时，技术支持人员通常会花一点时间一步一步地过一遍核对清单。一个典型的场景，在产品环境部署新的服务器或应用时，技术支持人员会花半天的时间来检查一遍系统在真实压力下的常见问题。该类核对清单是Ad hoc的，基于对该系统类型的经验和之前遇到的问题。

遇到问题时根据现象检查核对"FAQ"和"故障排查指南"就是使用了Ad hoc核对清单法。

科学法

科学法研究未知的问题是通过假设和实验进行的。总结下来有以下步骤：

1. 问题
2. 假设
3. 预测
4. 试验
5. 分析

问题就是问题的陈述，参考问题陈述法。从这点你可以假设问题的原因可能是什么。然后你进行实验，可以是观察性的也可以实验性的，看看基于假设的预测是否正确。最后是分析收集的试验数据。

举个例子，你可能发现某个应用程序在迁移到一个内存较小的系统时其性能会下降，你假设导致性能不好的原因是较小的文件系统缓存。你可以使用观测的试验方法分别测量两个系统的缓存失效率，预测内存较小的系统缓存失效率更高。用实验的方法可以增加缓存大小(加内存)，预测性能将会有所提升。另外，还可以更简单，实验性的测试可以人为地减少缓存的大小(利用可调参数)，预计性能将会变差。

网络故障排查

2

目录:

无法访问A2000-E 运维管理系统的对外服务

无法访问A2000-E 运维管理系统对外的服务，例如Web服务（80、443端口）、字符服务（22端口）、图形会话回放（5899端口）、后台管理（8022端口）

客户端到A2000-E 运维管理系统的网络异常

- 检查本地PC的网络配置是否正常。
- 通过ping命令检查本地PC到A2000-E 运维管理系统的连通性。
- 通过traceroute、tracert等命令，进行路由路径检测。

客户端到A2000-E 运维管理系统的端口不通

- 通过telnet命令，进行端口测试。
- 查看本地PC到A2000-E 运维管理系统之间，是否有防火墙拦截。
- 通过tcpdump命令进行抓包，查看故障原因。

A2000-E 运维管理系统IP地址冲突

如果其它设备的IP地址和A2000-E 运维管理系统的IP地址冲突可能导致部分端口通，部分不通。

- 检查A2000-E 运维管理系统所在网段的交换机ARP表，确认是否存在冲突。

A2000-E 运维管理系统无法访问外部设备的服务

A2000-E 运维管理系统无法访问外部设备的服务，既包括操作员访问的目标设备的对外服务，也包括管理员配置的A2000-E 运维管理系统与外部系统的对接，例如邮件服务、ldap认证等。

A2000-E 运维管理系统到外部设备的网络异常

- 通过ping命令，检查到外部设备的连通性。

- 通过traceroute命令，进行路由路径检测。

A2000-E 运维管理系统到外部设备的端口不通

- 查看A2000-E 运维管理系统到外部设备之间，是否有防火墙拦截。
- 查看外部设备是否修改默认服务端口。
- 登录外部设备系统，查看端口监听情况。
- 登录外部设备系统，查看相应服务日志。

浮动IP无法切换

HA环境下，如果发生主节点切换，浮动IP无法切换成功。

MAC地址绑定导致

浮动IP地址绑定了之前主节点的MAC地址。

- 进行主节点的切换，看浮动IP是否只能存在于特定节点上。
- 询问网络管理员是否有针对A2000-E 运维管理系统配置了MAC地址绑定。

活跃的字符、图形会话异常断开

网络震荡

由于网络震荡，丢包率高等问题，造成活跃的字符、图形会话异常断开。

- 复现问题，并进行长ping测试。查看异常时间段内，网络是否出现震荡、丢包率高、延迟高等现象。
- 切换网络或者直连A2000-E 运维管理系统进行测试，看能否复现问题。
- 复现问题，并在在客户端、A2000-E 运维管理系统、目标资产处分别抓包，将抓包结果发送给技术人员分析。

安全设备拦截

活跃会话异常断开问题可能是安全设备拦截导致。

- 询问客户的网络管理员或安全管理员，近期是否有网络变更或新增安全设备。
- 切换网络或者直连A2000-E 运维管理系统进行测试，看能否复现问题。
- 复现问题，并在在客户端、A2000-E 运维管理系统、目标资产处分别抓包，将抓包结果发送给技术人员分析。

业务故障排查

3

目录:

AccessClient

AccessClient调用异常

通过AccessClient调用本地应用程序异常。

软件安装不完全

操作系统、安全软件可能会对AccessClient的安装过程进行拦截，导致软件安装不完全。

- 尝试以管理员身份重装AccessClient，观察安装过程有没有被拦截。
- 打开安全软件的管理页面，查看黑名单列表中是否有AccessClient相关程序。
- 更换另外环境的一台PC，尝试使用看是否正常。

客户端关联错误

在第一次使用AccessClient关联客户端应用时，关联了错误的客户端应用，使之后的每一次访问都是请求错误的客户端应用。

- 移走文件，使AccessClient重新关联应用。
  a) 找到关联错误的客户端的EXE文件，将其移到其他目录。
  b) 通过Web页面访问该资产。在出现的选择客户端的弹窗中，选择正确的客户端应用。
  c) 将第1步中移走的错误客户端文件，还原回之前目录。
- 删除注册表中关联错误的键值。（请谨慎操作）
  a) 打开**运行**窗口。输入regedit，进入注册表管理。

b) 分别在**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths**和**HKEY_CLASSES_ROOT\Software\Microsoft\Windows\CurrentVersion\App Paths**路径下，寻找客户端程序名的键值。如果找到，删除该键值。

c) 通过Web页面访问该资产。在出现的选择客户端的弹窗中，选择正确的客户端应用。

Filefox浏览器关联AccessClient协议错误

浏览器使用URL为accessclient://xxx的方式调用本地的AccessClient。一般浏览器不允许修改此URL的调用的应用，但是Firefox可以修改。如果关联错误了，会造成所有打开的会话，都调用一个错误的应用。

- 修改Firefox的配置，调用AccessClient。
  a) 进入**选项** > **常规**。
  b) 在**应用程序**中找到**内容类型**为**accessclient**的条目，选择打开方式为**使用 访问客户端 处理（默认）**。
- 移走文件，使Firefox重新关联AccessClient。
  a) 找到关联错误的应用程序的EXE文件，将其移到其他目录。
  b) 通过Web页面访问任一资产，在出现的选择应用程序的弹窗中，选择**访问客户端**，并且勾选**记住我对AccessClient链接的选择**。
  c) 将第1步中移走的错误应用程序文件，还原回之前目录。

AccessClient访问时提示“请求的操作需要提升”

AccessClient打开相关客户端应用时，由于权限过低，无法打开该应用。需要修改客户端属性，使得打开该应用时，保持以管理员身份打开。

- 修改客户端属性。
  a) 右键单击应用程序，选择**属性**。
  b) 进入**兼容性**标签页，勾选**以管理员身份运行此程序**。单击**更改所有用户的设置**，勾选**以管理员身份运行此程序**。单击**确定**。
- 如果使用的是绿色版的客户端软件，请卸载该软件，并使用安装版本的软件。

操作员访问，页面始终提示安装AccessClient客户端

没有点击该提示的“已安装”按钮

该提示不会自动清除，如需清除，需要点击“已安装”按钮。

- 使用操作员登录系统，进入**访问资产**菜单。
- 如果页面左上角出现安装AccessClient的提示，点击**已安装**。

通过Firefox启动任意会话始终打开某一个客户端

使用Firefox在设备访问页面进行资产访问时，无论打开任何会话都是用特定的客户端打开，且无法成功登录。比如始终打开远程桌面客户端。

首次访问时没有选择AccessClient作为客户端

Firefox中首次访问时会要求选择客户，正常情况下应该选择"访问客户端"，有些客户可能会根据要访问的会话类型选择远程桌面客户端。

- 在Firefox的**首选项** > **应用程序**中找到accessclient。
- 单击accessclient对应的操作，在下拉菜单中选中**使用 访问客户端 处理（默认）**。

Web页面

页面加载速度慢

登录的页面，页面能够加载成功，但是加载速度缓慢。

网络异常

网络质量差、安全设备过滤、证书等问题会导致此现象。

- 通过Ping命令，检测本地PC到A2000-E 运维管理系统之间的网络。可以指定Ping包的大小，来测试大包的响应。如果出现丢包率高、延迟率高等问题，则需要注意。
- 询问客户的网络管理员或安全管理员，近期是否有网络变更或新增安全设备。

某个网页资源加载速度慢

网页通过加载资源来渲染页面，如果某个关键性的资源加载速度慢时，会导致整个页面加载慢。

- 尝试更换浏览器访问，看加载速度是否有提升。
- 按下F12激活开发者调试工具，选择**Network**页签，再次访问之前访问慢的页面，在**Network**中查看关于该网页的请求、响应信息。看哪个资源的加载最占用时间。

页面显示不正常

登录的页面，页面加载不完整，或者显示不正常

浏览器缓存问题

如果最近进行过升级，可能是因为浏览器中的css或者js有缓存导致的。

- 尝试清理浏览器缓存后，重试。

系统返回的资源文件有问题

排除缓存问题的话，可能是系统返回的资源文件就有问题。

- 开启浏览器的开发者模式（F12），检查console和network中是否有错误。

身份验证

错误的帐号名或密码

web页面提示"用户名或者密码错误"

用户不存在

输入的用户名错误，系统中不存在。

- 检查输入的用户名是否正确，管理员可以在**用户** > **用户列表**中查看系统中全部用户。
- 输入正确的用户名或者向管理员申请创建新用户。
- 使用第三方身份验证的，请检查ldap、radius上是否存在对应的账号。

密码错误

输入的密码错误

- 请检查输入的密码是否正确。
- 使用第三方身份验证的，可以检查ldap、radius上的相关日志。
- 如果忘记密码，管理员可以在**用户** > **用户列表**中重置该账号的密码。
- 如果超级管理员密码遗忘，可以在Console控制台菜单的**R.Reset admin**中重置。

无法连接第三方身份验证系统

使用LDAP或Radius身份验证时，系统无法连接身份验证服务器。

这种场景下，为了安全，系统不会明确提示是否是第三方身份验证系统故障。

- 如果管理员也无法登录时，可以在Console控制台菜单的**R.Reset admin**中重置管理员密码，重置后管理员的身份验证方式将被修改为本地密码验证。
- HA部署模式的需要确保系统所有节点和身份验证系统的通讯正常。
- 如果故障和网络无关，请检查第三方身份验证系统本身的可用性。

一次性口令已经被使用过

使用TOTP认证的，每一次性口令只能使用一次。

- 输入新的一次性口令。

时间不同步

使用TOTP认证时，系统与令牌的时钟不同步。

- 管理员可以在**系统设置** > **系统** > **基本设置** > **系统时间**中检查系统时间是否正确，如果不正确可以进行调整后再试。
- 可以尝试在**系统设置** > **用户** > **登录认证** > **动态令牌**中同步。如果同步后依然无法使用，请考虑更换令牌。

用户状态异常

Web登录时报"用户状态异常"

用户账户被禁用

管理员禁用了用户帐号

- 管理员可以在**用户** > **用户列表**中通过**筛选**查看已禁用用户，并取消禁用状态。

用户账户过期

用户帐号超过了管理员设定的有效期

- 管理员可以在**用户** > **用户列表**中通过**筛选**查看已过期用户，并重新修改有效期。

禁止登录

Web登录时登录时报“禁止登录”，SSH登录时报“认证失败”

来源IP或者登录时间不符合管理员设置的规则。

- 使用超级管理员身份登录web界面在**系统设置** > **用户** > **登录控制**查看是否设置了全局登录控制规则。
- 使用安全保密管理员身份登录web界面在**用户** > **用户列表**中查找到用户，在**编辑** > **高级**中检查**用户登录控制**相关的设置。

用户已经在x.x.x.x登录

登录时报"用户已经在x.x.x.x登录"

管理员设置了同一用户帐号同时只允许从一个IP地址访问。

- 根据提示IP在已登录的设备上注销所有会话，包括web、ssh。
- 也可以等待已登录的会话自动超时。
- 管理员也可以在**系统设置** > **资产** > **访问设置** > **所有会话**中禁用"同一用户帐号同时只允许从一个IP地址访问"。

- 管理员也可以在**系统设置** > **资产** > **访问设置** > **所有会话**中设置**WEB超时时间**，并且设置**会话切断策略**为切断。以使得超时会话自动断开。

登录很慢

登录过程缓慢，输入用户名和密码后需要很久才能加载，或者加载不了。

网络延迟高

- 使用ping检查客户端到服务器之间的网络延迟是否高。
- 在IE或者Chrome中可以按F12键打开开发者模式，重新访问一次，在**network**中检查页面资源的加载速度。

SMTP服务器故障

配置了身份验证E-mail告警，但是用于发送邮件的SMTP邮件服务器故障。

- 管理员可以在**系统设置** > **系统** > **基本设置** > **告警事件**中检查是否启用了**通知邮件事件来源**中的**身份验证**。取消设置可以解决问题。
- 管理员可以在**系统设置** > **系统** > **基本设置** > **邮件服务**中单击**测试**检查邮件服务器。

账号被锁定，请xx秒后重试

同一个客户端的登录错误次数过多，导致该IP被锁定。

- 请排查本机是否登录错误次数过多。
- 请查看本机到目标设备的网络，是否有过NAT。如果同一个NAT出口的IP被大多数内网地址使用，可能很容易达到客户端锁定次数。

访问权限

访问看不到资产

操作员在**访问资产**页面看不到相应资产。

没有配置访问权限

- 安全保密管理员可以在**权限** > **权限查看** > **按用户**处过滤该操作员，查看是否有相应权限。

变更单或者工单超出时间范围

- 在变更单权限下，安全保密管理员可以在**权限** > **权限配置** > **变更单**中查看相应变更单时间范围，确认没有超出时间范围。

- 在工单权限下，安全保密管理员可以在**工单** > **工单管理** > **已办工单**中查看相应工单的时间范围，确认没有超出时间范围。
- 安全保密管理员可以在**权限** > **权限查看** > **按用户**处过滤该操作员，查看是否有相应权限。

变更单被禁用

- 安全保密管理员可以在**权限** > **权限查看** > **按用户**处过滤该操作员，查看是否存在被禁用的变更单。
- 安全保密管理员可以在**权限** > **权限配置** > **变更单**中，筛选状态为禁用的变更单进行查看。

规则模板开启禁用

- 在动态权限下，安全保密管理员可以在**权限** > **权限配置** > **动态权限**处查看相应权限的规则模板的控制策略是否为禁止访问。
- 在变更单权限下，安全保密管理员可以在**权限** > **权限配置** > **变更单**中找到相应权限，查看变更单中的规则模板的控制策略是否为禁止访问。
- 在工单权限下，所有的工单的规则模板都是缺省的模板。

规则模板开启时间范围或IP范围

- 安全保密管理员可以在**权限** > **权限配置** > **规则模板**处，点击相应规则的**规则管理**，查看时间范围和IP范围。

资产没有协议，或者协议被禁用

- 安全保密管理员可以在**资产**处，编辑相应资产，进入**访问协议**，查看是否不存在协议，或者协议被禁用。

资产被禁用

- 安全保密管理员可以在**资产**处，查看是否资源被禁用。

访问资产时，出现“操作失败”提示

访问资产，出现“操作失败”提示，具体内容为:失败: 无权访问资产，请确认 1、访问规则是否配置 或 登录模板时间和ip范围是否允许；2、是否存在异常的会话复核； 3、 检查当前用户状态是否异常。

访问权限已去除资产，但是访问资产页面未及时刷新

- 刷新访问资产页面，查看相应资产是否消失。

访问存在会话复核时，唯一的复核人被禁用或者被删除

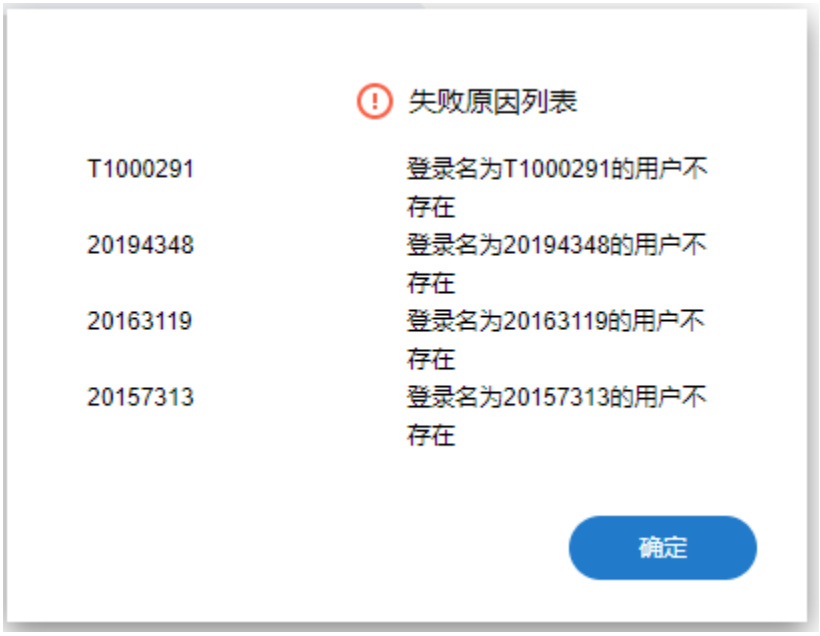
- 安全保密管理员进入**高危操作** > **会话复核**，查看相应会话中的复核人是否被禁用或者删除。

用户状态被禁用;密码过期、帐号过期

- 超级管理员进入**用户** > **用户管理** > **用户列表**，通过筛选角色的属性来过滤出**禁用**、**密码过期**、**账号过期**的账号。

上传变更单，出现资产名/用户名不存在

上传变更单时，报错如下:



系统不存在相应的用户或资产

- 超级管理员进入**用户**、**资产**菜单，查看相应用户、资产是否存在。

访问看不到字符资产的SFTP服务

访问时，能够看到字符资产，并看到该资产下的SSH服务。但是看不到SFTP服务。

访问权限中关联的账号没有托管密码

登录目标资产的SFTP服务，必须以预配置账号、密码的方式。如果访问权限中关联的账号没有托管密码，则SFTP服务无法使用。

- 查询相关权限中关联的系统账号，并到资产配置中查看相应账号是否有托管密码。

命令权限

命令权限不生效

配置了命令权限，但是命令权限并没有生效。

命令权限的匹配不准确

命令权限使用正则表达式进行匹配，正则表达式规范请参考http://tool.oschina.net/uploads/apidocs/jquery/regexp.html

- 可以在http://tool.oschina.net/regex/进行正则表达式准确性测试。

命令权限的匹配顺序不正确

命令权限中的多条规则按照从上至下，从高到低的优先级进行匹配，并且只执行匹配的第一个规则的动作。

- 尝试修改命令的顺序，查看是否匹配成功。

命令权限的生效时间不匹配

如果命令权限中有配置生效时间，需要保证是在生效时间段内操作。

- 使用超级/安全保密管理员进入**高危操作** > **设置** > **高危命令**，编辑相应的高位命令，查看生效时间范围。

XDMCP和Xfwd

访问xdmcp会话黑屏

网络异常

开启xdmcp会话，需要先访问目标资产的UDP177端口。随后目标资产会反向连接A2000-E 运维管理系统6000-6999之间的TCP端口建立xdmcp会话。

- 查看目标资产UDP177端口是否有监听。
- 查看A2000-E 运维管理系统是否有监听6000-6999端口。
- 查看网络路径中是否有防火墙拦截。
- xdmcp会话的双方都不能穿越NAT，请确认A2000-E 运维管理系统到目标设备之间没有NAT设备。

A2000-E 运维管理系统多网卡导致

当A2000-E 运维管理系统发送xdmcp request时，会发送本地所有的IP地址到目标资产，如果目标资产选择了不可通信的IP进行display的回连，会出现此问题。

- 在A2000-E 运维管理系统端抓包，看目标资产回连的数据包请求的display的IP地址是不是错误的。

访问xfwd会话闪退

通过H5模式启动的xfwd会话，在新窗口启动后闪退。

SSH服务异常、账号错误

xfwd依赖于该资产的SSH服务，需要确保SSH服务能够通讯正常。并且使用的账号密码正确，能够使用SSH协议登录目标资产。

- 检查目标设备是否有修改SSH服务的默认端口。
- 通过telnet命令测试目标资产的SSH服务端口的连通性。
- 在A2000-E 运维管理系统的**资产**处，进行该资产的相应账号SSH协议的登录测试。

使用的xfwd命令或参数错误

- 使用**xstart**工具直连目标资产，使用相同的xfwd命令和参数，测试是否连接成功。

目标资产SSHD服务没有支持X11forwarding

使用xfwd功能，需要目标资产的SSHD服务开启X11forwarding。

- 使用**xstart**工具直连目标资产，测试是否连接成功。
- 查看目标资产的SSHD配置文件，查看是否有设置**X11Forwarding yes**。

访问xdmcp会话乱码

访问xdmcp会话，会话中部分或全部文字显示乱码。

A2000-E 运维管理系统中的X11协议不存在该字体，需要手工增加

1. 问用户能否提供目标资产相关的字符集。
2. 按照客户提供的字符集安装方式进行安装。

网盘

看不到文件传输菜单或者没有上传下载按钮

进入文件传输后只能看到我的文件，或者没有上传下载按钮。

没有权限

如果用户账户没有对任何资产的文件传输权限时进入文件传输只能看到我的文件。

- 管理可以在**权限**中修改用户的权限设置。

文件大小超出配置文件设定值

上传文件到网盘时提示“文件大小超出配置文件设定值”或者“文件大小不可超过xxx”。

上传文件大小系统允许的最大值

- 系统默认允许上传10240MB的文件。

被网络设备拦截

如果没有达到设定的限制也出现这类错误，可能被WAF、IPS防火墙等设备拦截

- 在客户端PC上的cmd中执行tracroute <堡垒机IP>命令。
- 根据tracroute的返回经过的网络设备是否会对http的Body Size进行限制，或者是否会拦截大流量的http请求。

资产拒绝连接

选择目标资产后提示

```
资产拒绝连接
```

连接目标资产的sftp端口是被拒绝

- 检查目标资产的主机防火墙设置及其它可能的黑白名单设置。
- 检查目标资产与A2000-E 运维管理系统之间的防火墙设置。

资产连接超时

选择目标资产后提示

```
资产认证超时
```

目标资产异常

资产认证超时说明可以连接目标资产，当时尝试进行身份认证时超时，通常是目标资产存在异常。

- 检查目标资产的/etc/ssh/sshd_config中的UseDNS设置，可以尝试设置成NO，并重启sshd服务。
- 检查目标资产的系统负载。
- 检查目标资产的磁盘空间。

网络异常

网络存在丢包或者延迟高也有可能导致该问题。

- 使用ping命令，进行网络诊断。

密码或密钥错误

选择目标资产后提示

```
密码或密钥错误
```

文件可能被管理员删除中托管的目标资产的用户名或者密码密钥错误

- 管理员可以在**资产**中进行登录测试。

改密和帐号管理

无法创建改密计划

创建改密计划时，系统提示**不允许新建改密计划：系统中需存在配置ZIP文件密码或者PGP公钥和邮箱的用户**

创建改密计划前，需要配置前提条件

创建改密计划，需要系统的超级管理员或安全保密管理员已配置zip密码或PGP公钥，并配置该用户的邮箱。

- 使用超级管理员或安全保密管理员进入**帐号设置**。
- 进入**个人设置**，配置**工作邮箱**。
- 进入**信息加密**，配置**ZIP文件密码**或**PGP公钥**。

改密计划执行失败

改密计划已经创建，但是执行后，提示改密计划执行失败。

密码备份失败

为防止密码丢失，A2000-E 运维管理系统在改密前，会进行密码的备份操作。如果密码备份失败，改密不会进行。

密码备份策略可以同时指定多种密码备份方式，只要任一方式备份成功，则会进行改密。如采用密码分段方式，需要保证两断密码都备份成功。

- 使用超级管理员，进入**系统设置**，点击**基本设置** > **邮件服务**。点击**测试**，填写收件人的邮箱。测试邮件是否发送成功。
- 使用超级管理员，进入**系统设置**，点击**基本设置** > **文件服务**。点击**测试**，查看是成功。

没有可改密的帐号

在改密计划的关联帐号处，没有指定帐号，或者动态关联的规则没有匹配到帐号。

- 使用超级管理员或安全保密管理员进入**帐号管理**，点击**改密计划**，编辑相应的改密计划，点击**关联帐号**，查看指定帐号是否为空。或者点击**动态关联**，点击**查看帐号**，查看关联帐号是否为空。

上一次改密失败，不可再改密

A2000-E 运维管理系统出于对密码安全的考虑，在改密失败后，不可直接进行下一次改密。如需进行改密，需要进行登录测试以确认密码。

- 使用超级管理员或安全保密管理员进入**帐号管理**，选择相应的资产，在帐号列表中选择相应的帐号，点击**编辑**。点击**密码管理**，点击**登录测试**。出现**登录成功**弹窗，代表确认密码。

目标资产缺少相关协议或协议被禁用

字符资产的改密需要资产处拥有Telnet或者SSH协议，并且该协议没有被禁用。

- 使用超级管理员或安全保密管理员进入**资产**，选择相应资产，查看相应协议是否存在，或者是否被禁用。

字符资产改密失败

不支持的设备类型

A2000-E 运维管理系统支持改密的主机字符资产只有**Linux**。网络字符资产包括**H3C Comware、Huawei Quidway、General Network** 。

- 当待改密资产不满足上述资产类型要求时，建议通过自定义改密方法来解决。

改密会话登录失败

改密需要A2000-E 运维管理系统使用SSH/Telent协议登录到字符资产。如果改密会话登录失败，则改密也会失败。

- 在**帐号管理**处，进行字符资产的登录测试，查看是否成功。
- 如果是因为登录过程的交互存在问题，导致登录会话失败，可以通过**资产适配**功能进行提示符或者命令的适配。

没有托管特权帐号、待改密帐号的密码或托管密码错误

字符资产改密要求A2000-E 运维管理系统托管了特权帐号密码，或托管了待改密帐号密码。

- 查看**帐号管理**中的相应资产，编辑相应帐号，点击**登录测试**，查看登录测试是否正常。

改密的交互步骤不一致

字符资产改密的逻辑是A2000-E 运维管理系统使用SSH/Telent协议登录到字符资产后，执行passwd命令进行交互式的改密操作。当目标资产的passwd的交互过程和标准Linux的不一致，则会出现改密失败。

标准Linux的特权帐号改密过程:

```
[root@node01 ~]# passwd xuhf
Changing password for user xuhf.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@node01 ~]#
```

标准Linux的普通用户改密过程:

```
[xuhf@node01 ~]$ passwd
Changing password for user xuhf.
Changing password for xuhf.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[xuhf@node01 ~]$
```

- 访问目标资产，执行passwd命令，查看改密的具体交互过程。查看是否与标准Linux的改密过程一致。
- 查看改密日志，是否有交互步骤出错的记录。
- 如果确认改密交互步骤与标准Linux的不一致，可以使用自定义改密方法。

密码复杂度不符合要求

如果目标资产有密码复杂度要求，设置简单密码时，将改密失败。

- 查看改密日志，是否有关于密码过于简单的提示。例如:**BAD PASSWORD: is too similar to the old one。**
- 尝试使用随机生成密码的策略，以使密码满足复杂度要求后，重新进行改密尝试。

改密过程交互过慢导致超时

A2000-E 运维管理系统改密过程中，会话的登录超时和每个步骤交互超时默认为20秒。如果会话登录或设备交互过慢会导致改密失败。

- 进行**帐号管理**中的相应资产的登录测试，查看登录测试是否过慢。
- 查看改密日志，是否有关于超时的提示。例如:**timeout when matching:**。
- 通过配置**资产适配**，修改**登录超时时间**。该配置影响登录超时以及每个步骤的交互超时。

目标设备编码为中文导致使用切换自方式改密失败

当目标设备编码为中文，在使用切换命令su后出现的密码提示为中文，导致匹配失败，从而改密失败。

- 通过**资产适配**，在帐号切换命令前指定系统编码。例如:**export LANG=C LC_ALL=en_US.UTF-8;su - root**。

英文语言环境设置失败

在使用默认脚本改密时，脚本会执行设置英文语言环境的语句，以使得当前会话的交互内容都为英文，来匹配所有的改密步骤。如果英文语言环境设置失败，可能会导致改密失败。

- 查看改密过程中是否包含中文，是否出现中文内容后，提示匹配超时信息。

自定义脚本改密失败

本故障排查针对的自定义改密脚本类型包括：Telnet、SSH。

需要转义字符没有被转义

改密脚本的**匹配**字段可以使用正则表达式进行匹配，当遇见某些特殊字符时，需要进行转义。

- 转义字符包括:**$ ( ) . * + [ ] ? \ ^ { } |**。转义方式为待转义字符前加反斜杠。例如:$需转义为\$。

收集日志

4

目录:

收集客户端日志

当出现访问异常时，请根据访问环境和方法选择收集相关的客户端日志来分析问题。

收集浏览器日志

当访问Web页面时异常时，请收集浏览器日志来分析问题。

收集项	收集方法
浏览器请求/响应信息	当出现页面加载不成功、页面部分元素加载异常、页面加载速度较慢等异常时，请收集浏览器的请求/响应信息，Chrome、Firefox和IE的收集方法都相同。 1. 打开浏览器，按下**F12**激活开发者调试工具。 2. 选择**Network**页签。 3. 再次访问之前出现异常的Web页面，在**Network**中查看关于该网页的请求/响应信息。
浏览器证书相关信息	请收集到浏览器证书信息、加密协议、密钥算法等信息，以Chrome为例。 1. 打开浏览器，按下**F12**激活开发者调试工具。 2. 选择**Security**页签，收集证书、加密协议、密钥算法等信息。

收集SSH客户端日志

当访问SSH会话异常时，请收集SSH客户端日志来分析问题。

收集项	收集方法
字符终端下SSH命令的连接日志	执行SSH命令时带上**-v**参数（**-v**代表verbose级别，最高为三级），例如**ssh root@1.1.1.1 -vvv**。
Xshell SSH连接日志	1. 打开Xshell软件，单击**文件** > **属性**，在出现的新窗口，单击**高级** > **跟踪**。 2. 勾选**SSH版本，算法交换和用户身份验证**。 3. 启动一个新的SSH会话，该SSH会话的连接日志会显示出来。

收集AccessClient日志

通过A2000-E 运维管理系统的Web界面启动的会话，会调用AccessClient工具，当访问资产异常时，请收集AccessClient的日志。

收集项	收集方法
AccessClient调用本地应用的日志	打开**此电脑**，在地址栏输入**%temp%**进入临时目录，找到**AccessClient.log**。

收集客户端软件版本信息

当通过客户端软件访问A2000-E 运维管理系统出现异常时，请收集客户端软件的版本信息，以便于搭建复现问题的环境。

收集项	收集方法
Windows软件版本	软件版本信息一般位于菜单栏**帮助** > **关于**中。
Linux软件版本	执行命令**dpkg -l |grep 软件包名称**查看软件版本，例如dpkg -l |grep openssh-client。

收集目标资产日志

当出现访问异常时，也可能是目标资产出现异常，请收集目标资产日志来分析问题。

收集Linux系统日志

当通过A2000-E 运维管理系统访问Linux设备异常时，请收集该Linux设备的日志来分析问题。

收集项	收集方法
message日志	该日志记录系统服务、kernel等信息。日志路径一般为/var/log/messages，该日志一般会以周为单位进行回滚，如有必要请收集所有时间戳的messages日志。
secure日志	该日志记录用户认证相关信息。日志路径一般为/var/log/secure，该日志一般会以周为单位进行回滚，如有必要请收集所有时间戳的secure日志。

收集A2000-E 运维管理系统日志

当出现访问异常时，可能是A2000-E 运维管理系统出现异常，请收集A2000-E 运维管理系统日志来分析问题。

收集会话操作日志

当访问目标设备出现异常时，可以通过收集会话操作日志分析问题。

收集项	收集方法
字符会话	字符会话日志通过Web页面收集。 **1.** 进入**审计**页面，单击**字符会话**。 **2.** 选择相应的字符会话，单击**更多**，单击**下载**。

收集项	收集方法
图形会话	图形会话日志通过Web页面收集。 **1.** 进入**审计**页面，单击**图形会话**。 **2.** 选择相应的图形会话，单击**更多**，单击**下载**。