某局点A2000-G堡垒机(611X)Agent方式Windows自动改密失败处理经验案例

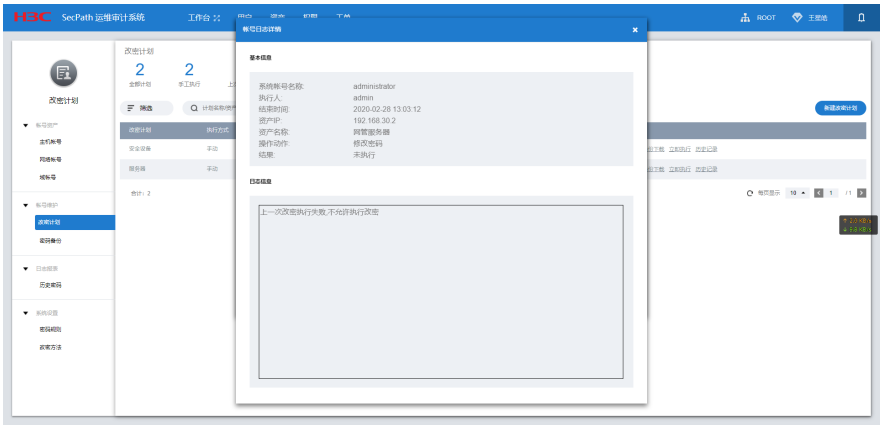
运维审计 堡垒机 **孙轶宁** 2020-03-30 发表

组网及说明

客户购买了一台A2000-G堡垒机做运维审计，版本是6112

问题描述

客户在配置**Agent方式**的Windows自动改密过程中，发现无法改密成功，出现如下图报错：上一次改密执行失败，不允许执行改密



过程分析

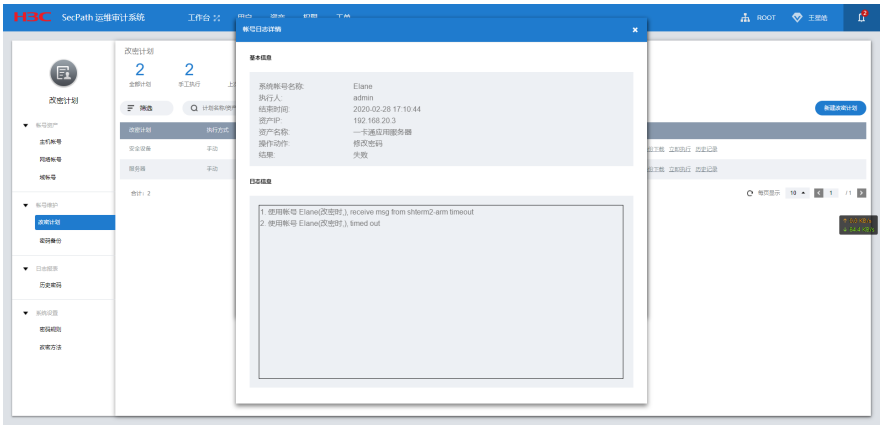
1、测试堡垒机和Windows服务器之间的连通性，发现没有问题。

2、测试堡垒机登陆Windows服务器，发现堡垒机能够通过RDP协议正常登录到Windows服务器，说明Windows服务器的账号密码均配置正确。

3、检查Windows服务器上Agent的配置，发现运维审计系统的IP地址和端口均配置正确，并且Windows防火墙也放通了Agent客户端。

4、查看配置指导，发现有这样一句话：如果目标设备上已安装Agent，且Agent上已配置运维审计系统的IP地址和端口（缺省端口是TCP 3301），**则不需要要目标设备在运维审计系统上托管密码。**再检查堡垒机的配置，发现堡垒机上托管了Windows服务器的密码。

5、删除托管的密码，再次尝试改密，仍然报错，但是报错变成了time out，如下图：



6、再次检查Windows服务器，发现服务器上安装了杀毒软件，并且在尝试改密的时候有拦截提示，在杀毒软件放行后，问题解决。

解决方法

Agent方式的Windows改密失败是有两个问题：

1、出现上次改密失败，不进行改密的报错是因为agent方式改密不能托管密码。

2、出现超时报错是因为客户电脑安装的杀毒软件拦截了改密操作，需要放行。