聚铭配置安全评估工具产品白皮书

南京聚铭网络科技有限公司

2016 年 11 月

联系信息

地　　址：南京市雨花区软件大道 180 号 07 栋 406 室

邮　　编：210000

电　　话：025-52205520 025-52205570

传　　真：025-52205565

邮　　箱：support@juminfo.com

网　　址：www.juminfo.com

全国服务热线：400-1158-400

目 录

1 安全运维面临的问题

随着信息化建设地深入发展、设备种类不断增加，安全配置管理问题日渐凸出。为了维持IT 信息系统的安全并方便管理，管理员必须从入网审核、验收、运维等全生命周期各个阶段加强和落实安全要求，同时需要设立满足安全要求的基准点。

针对行业的业务系统建立安全检查点与操作指南的基准安全标准，则成为各个行业安全管理人员最为紧迫的事情。但目前面临如下问题：

1.1 设备及应用种类繁多、工作量巨大

安全运维人员需要面对种类繁多的设备或应用，如何管理这些设备和应用的配置，或者如何定位知道这些设备配置的安全问题，是他们在安全运维过程中遇到的巨大问题和挑战。

而且，由于需管理的设备分布范围广、分属不同的业务系统，如何能快捷、方便的收集和分析这些配置，则成为横亘在安全运维人员面前的一个巨大难题。

一般而言，日常运维人员需要收集和分析各种主机系统、网络设备、数据库系统以及其它中间件（如 Tomcat、Apache 等）的配置；这些配置的收集和分析存在以下问题：

1. 部署位置多种多样
2. 配置的表现形式和存储样式不尽相同，如有的在配置文件中、有的在注册表中；有的配置文件是一般文本，而有的又是 XML 形式
3. 采集过程中可能还需要穿越网关设备或堡垒主机
4. 采集时还需要一些辅助的命令或设置，如采集 Oracle 时，需要知道实例名等
5. 由于配置在形式上存在千差万别，如何准确地分析则成为困难的事情

1.2 标准难于统一

目前，由于业界还没有形成统一的配置问题审计的行业标准，因此各家提出的标准也是不一而足，而且这些标准也是被频繁地修改，造成维护和定位困难；一般用户很难自己去跟踪和修订标准。

就当前而言，我们能接触到的标准就包括了 CIS（来自美国）、中国移动管信、中国移动网络、中国电信以及聚铭内部标准；这些标准不仅在支持的设备类型和应用类型上存在差异，就是针对几乎相同的检查点（配置项）而言，做法也不尽相同。

上述的差异造成研究、开发、维护安全配置基线是一项工作量巨大的任务。

1.3 自动化程度低

以往，对于设备或应用的配置审计，一般都是通过人工方式进行，仅在上线前进行一次评估（安全加固），这样做的缺点是显而易见的：

1. 纯粹依赖手工方式，效率低下

2. 在设备或应用上线后，不能定时地或经常性地进行评估，从而无法反映现网设备或应用的配置情况，这导致系统存在巨大的安全隐患（如未能按口令复杂度设置管理员账号）

3. 结果比较零散，只能依赖于人工汇总

2 安全基线的支持

2.1 支持的安全基线种类

聚铭配置安全评估工具支持的设备系统类型和应用系统类型如下所示：

1. 支持 Windows XP/2003/Vista/7/2008/8/10
2. 支持 Linux（CentOS、Red Hat、SUSE）
3. 支持 AIX
4. 支持 Solaris
5. 支持 HP-UX
6. 支持 Cisco 路由器的主流产品
7. 支持 Juniper 路由器的主流产品
8. 支持华为路由器的主流产品
9. 支持 Oracle
10. 支持 MS SQLServer 2000/2005/2008
11. 支持 MySQL
12. 支持 Tomcat
13. 支持 Apache
14. 支持 IIS
15. 支持 Weblogic

2.2 采集方式

一般而言，除 Windows 系统外，聚铭配置安全评估工具所采用的采集方式为远程形式，用户不用在目标系统上安装任何应用。

远程采集的口令、账号、管理员口令、管理员账号等相关登录信息可保存在外部文件中（已加密），也可以临时输入。

采集的配置信息和最终的分析报告也可被存储在外部任务文件中，供今后分析或导出使用。

2.3 与安全管理中心的集成

聚铭配置安全评估工具的执行结果可被导出到外部文件中，这种文件的格式可被聚铭网络的安全运营中心所识别和保存。

3 功能概述

3.1 功能架构概述

聚铭配置安全评估工具主要包括三个模块：

1. 任务管理：包括新建任务和任务导入管理；能建立或 导入历史上保存的配置收集和分析任务；

2. 报告分析：可以合并多个已执行完毕或比较两个执行完成的任务

3. 配置：提供一些系统工具，包括口令文件管理（用户可以预先编辑口令、账号等登录信息）、脚本管理、跳转设置等。

上述各功能详述如下。

3.2 任务管理

1. 新建任务

新建任务以向导方式呈现，向导共五页，且向导每一步均提供“保存”、“另存为”功能，首次“保存”和“另存为”功能相同：

■ 定义配置收集任务：定义任务的基本信息，即定义任务名称、收集的对象（IP 地址）

- 口令设置：设置对象的口令等登录信息

- 检查配置是否完整：检查任务中的各个对象的信息是否已经被设置完整，这些信息包括账号口令、使用策略、对象类型；在本页还可以另行添加对象并进行批量的登录检测

- 信息核对：核查任务的信息是否已经设置完整

■ 任务执行结果：生成任务检查报告并可导出

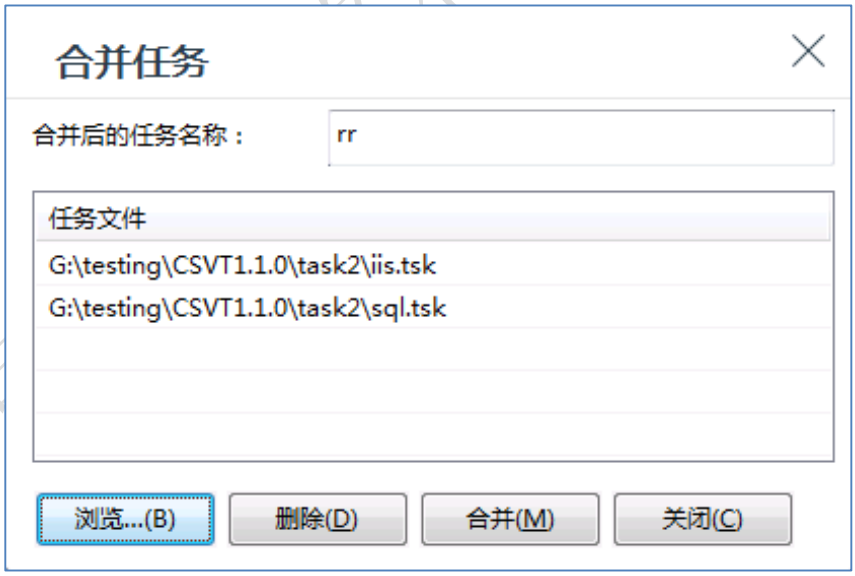
2. 导入任务

可以将以前保存的任务系统导入到工具中：

3.3 报告分析

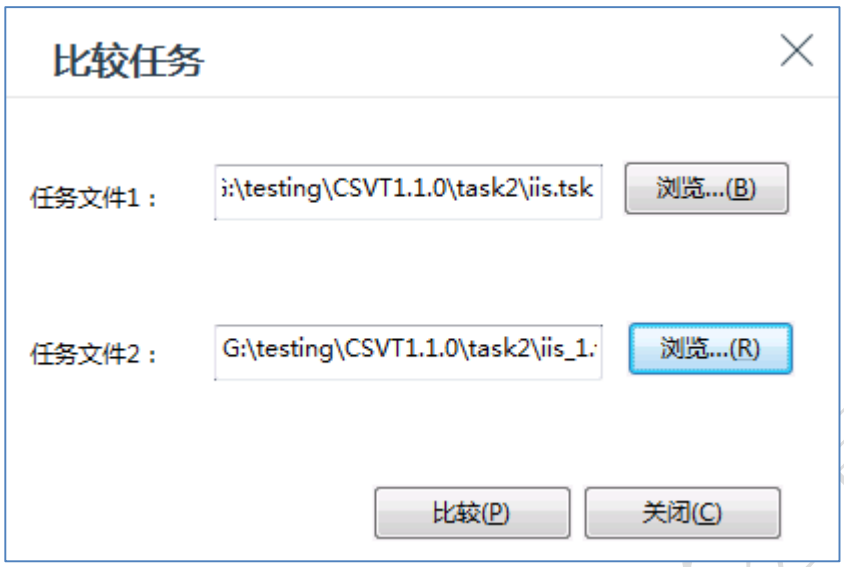
1. 合并报告

合并多个历史上执行完毕的任务：



2. 比较报告

比较两个历史上执行完毕的任务；比较的主要目标是具备相同 IP 及类型的对象及其检查结果：



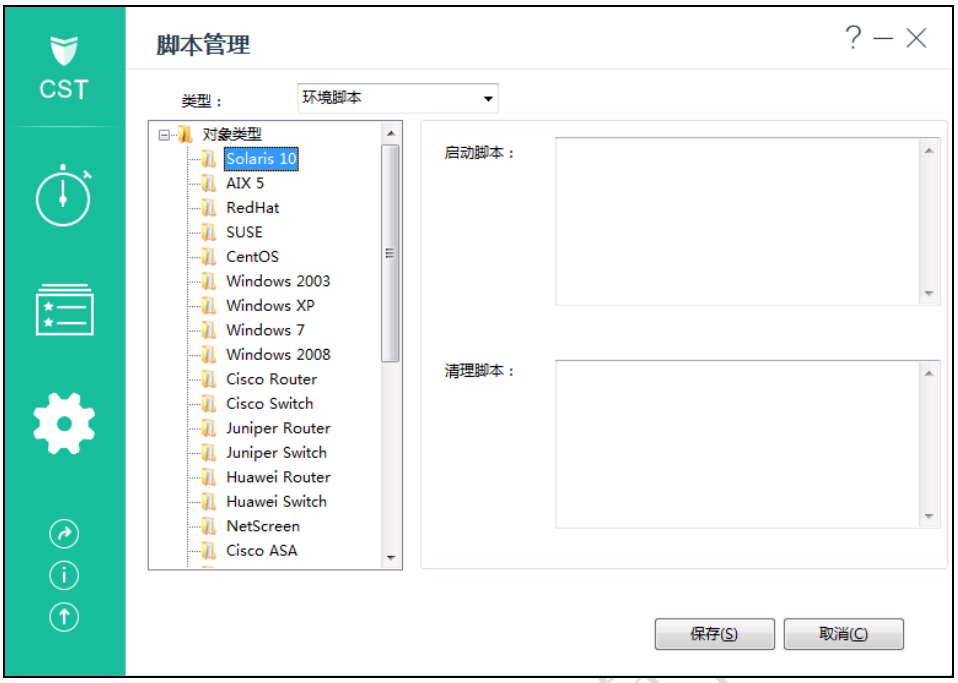
3.4 配置

1. 口令文件

新增、编辑、修改口令文件；口令文件中主要包括若干条登录信息；登录信息包括：登录账号、口令、管理员账号（可选）、管理员口令（可选）、登录方式、登录端口：

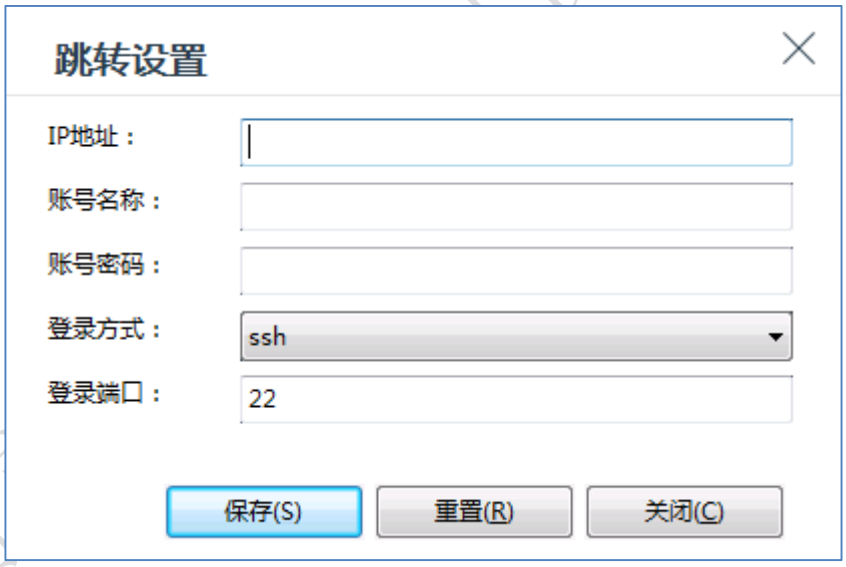
2. 脚本管理

可按对象的类型增加和修改其启动脚本（在执行收集前运行）和清理脚本（在收集完毕后运行）：



3. 跳转设置

如果不能直接采集目标设备信息，则可以设置中间的跳转服务器进行。



4 产品优势

聚铭网络提供了业界领先的安全配置审计解决方案，其解决方案的主要优势体现在：

4.1 多标准的支持

目前，聚铭配置安全评估工具不仅支持聚铭配置基线标准，还支持中国移动的配置基线标准、中国电信配置审计基线标准；今后仍将持续关注各种标准的发布和实行，严密跟踪各种标准的发布和变化。

4.2 对象类型的自动探测

无需用户手工配置检查对象的类型，本工具可以自动探测其类型（不仅是操作系统，也可探测应用的类型）且准确率较高。

4.3 对象登录验证

支持批量和单个对象的登录验证，并将验证结果直接显示在工具的界面上。

4.4 便捷的使用方式

聚铭配置安全评估工具是基于 Windows 平台开发的，您可以在 WindowsXP/Windows2003/Windows Vista/Windows 7/Windows2008 等 Windows 系统上使用；无需在目标设备上安装其他应用；U 盘型式即插即用。

4.5 检查的速度较快

由于聚铭配置安全评估工具采用特殊的并发算法，与其它同类产品相比，检查和分析速度较快，能在较短的时间内得到结果和报告。