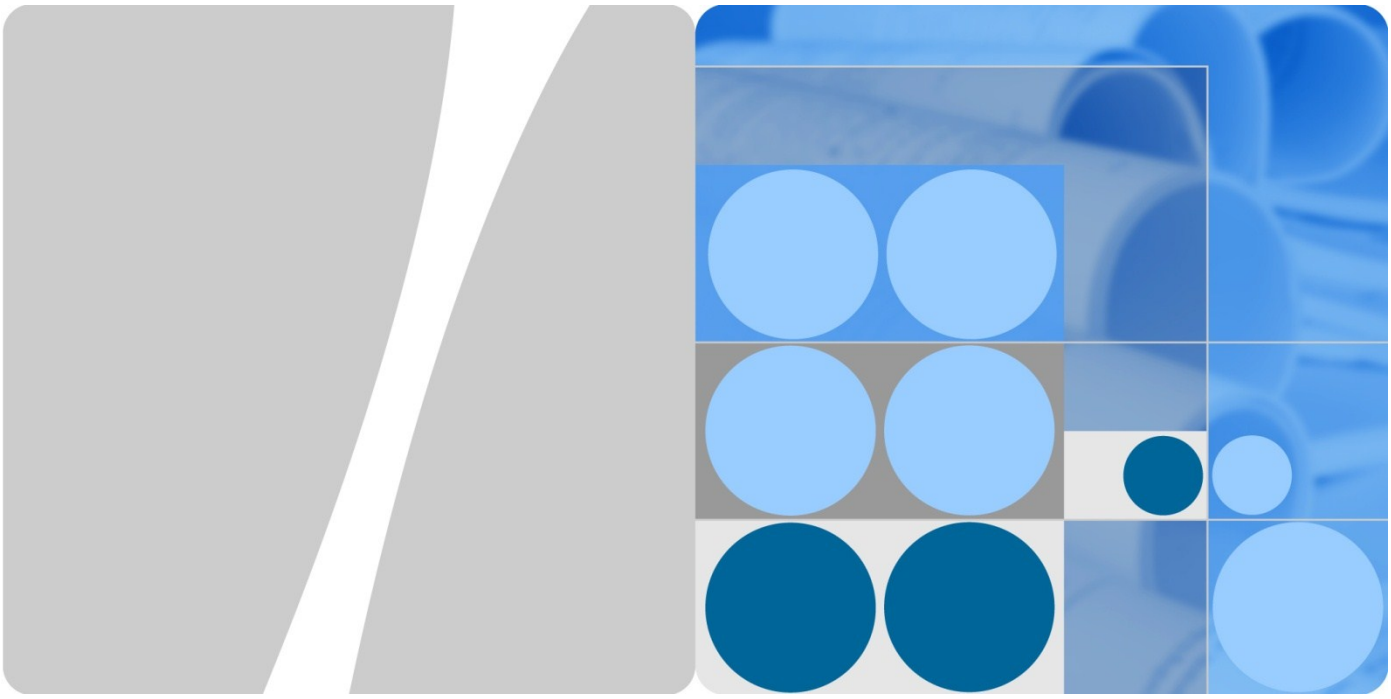


华为 UMA 统一运维审计产品特性描述

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

目 录

1 命令审计特性

命令审计特性由这些部分组成：SFTP 传输审计、字符终端审计、图形终端审计、改密日志审计、事件日志审计、登录日志审计、配置日志审计、日志情况总揽、综合日志报表。

1.1 SFTP 传输审计

SFTP 方式传输文件的过程被统一安全管理与综合审计系统完整记录，方便后期集中审计，责任鉴定。如下图：

日志详情，见下图：

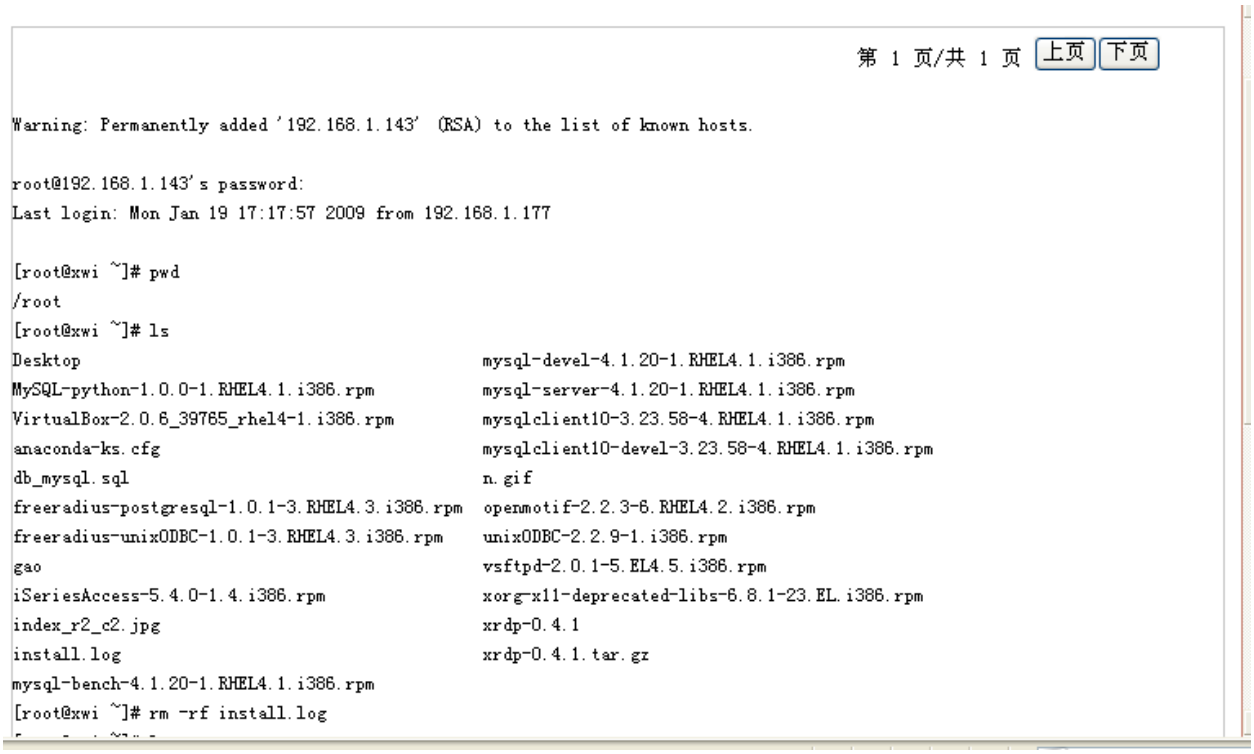
1.2 字符终端审计

“字符终端令审计”对登录到主机资产服务器上的用户操作命令和命令结果进行实时审计。如下图：

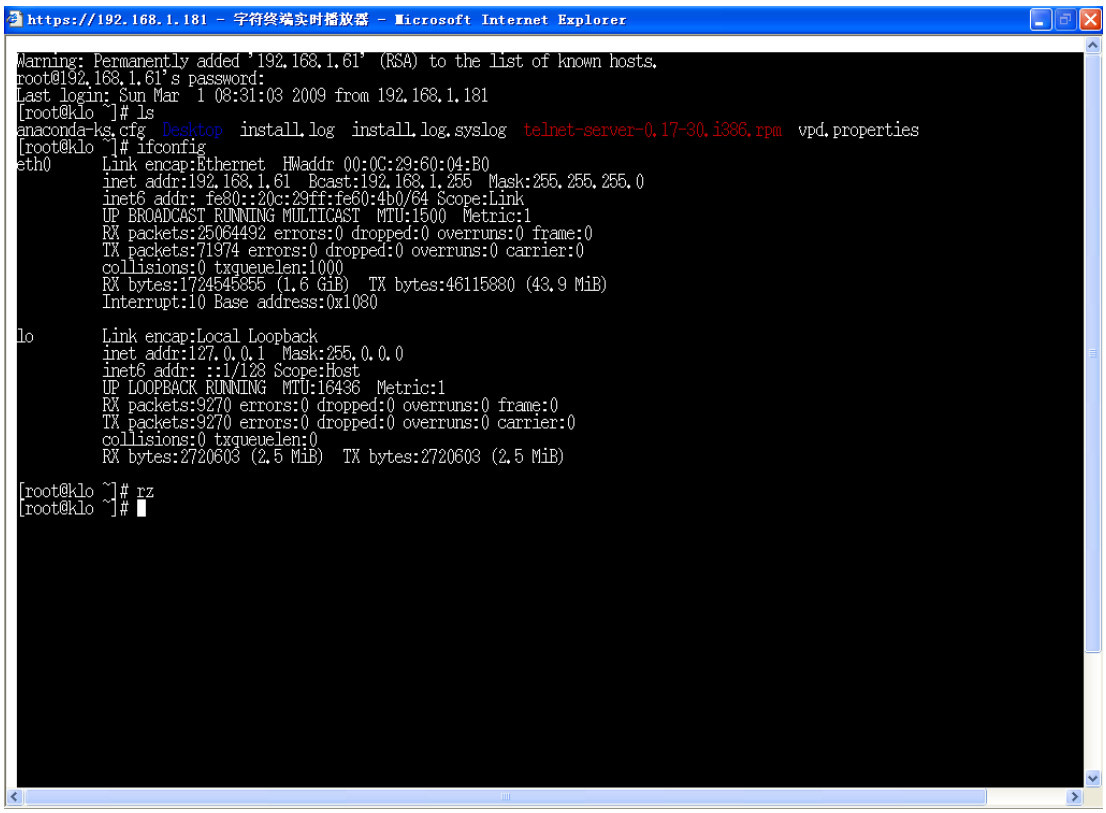
用户可以根据主机地址、起始日期、结束日期、网关用户、登录地址、用户命令、主机帐号、操作时间这些参数进行挑选来进行有目的的审计，根据审计情况即时修改策略配置使得主机资产服务器更加安全和合理的被使用。例如：审计用户操作命令 rm -rf 的操作纪录，在“用户命令”文本框中输入命令 rm -rf，点击确定按钮后显示结果为下图所示：

点击序号 1 对应记录命令查看项的“命令”超级链接，结果显示如下图：

点击实“时命令审计”对应记录“屏幕”项的超级链接，结果显示如下图：

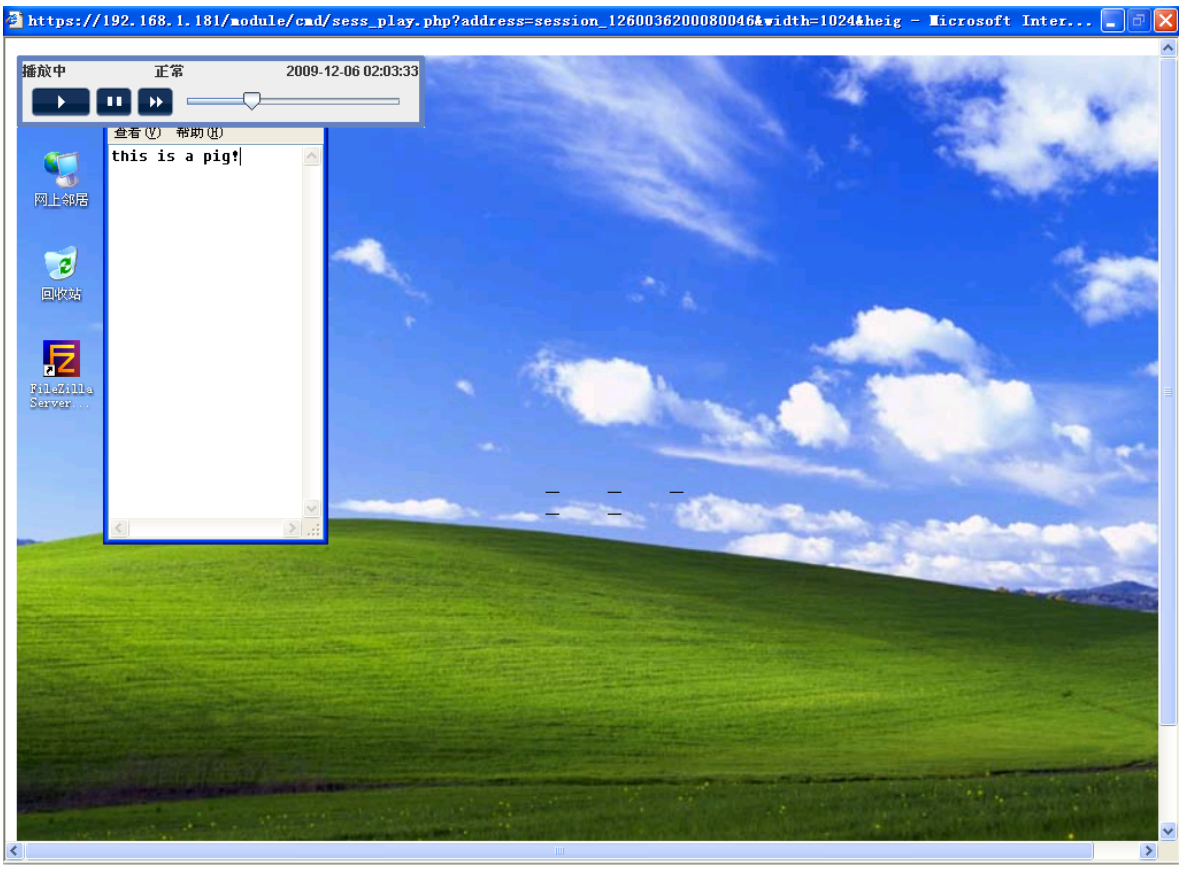


点击“播放”超级连接，结果如下图：

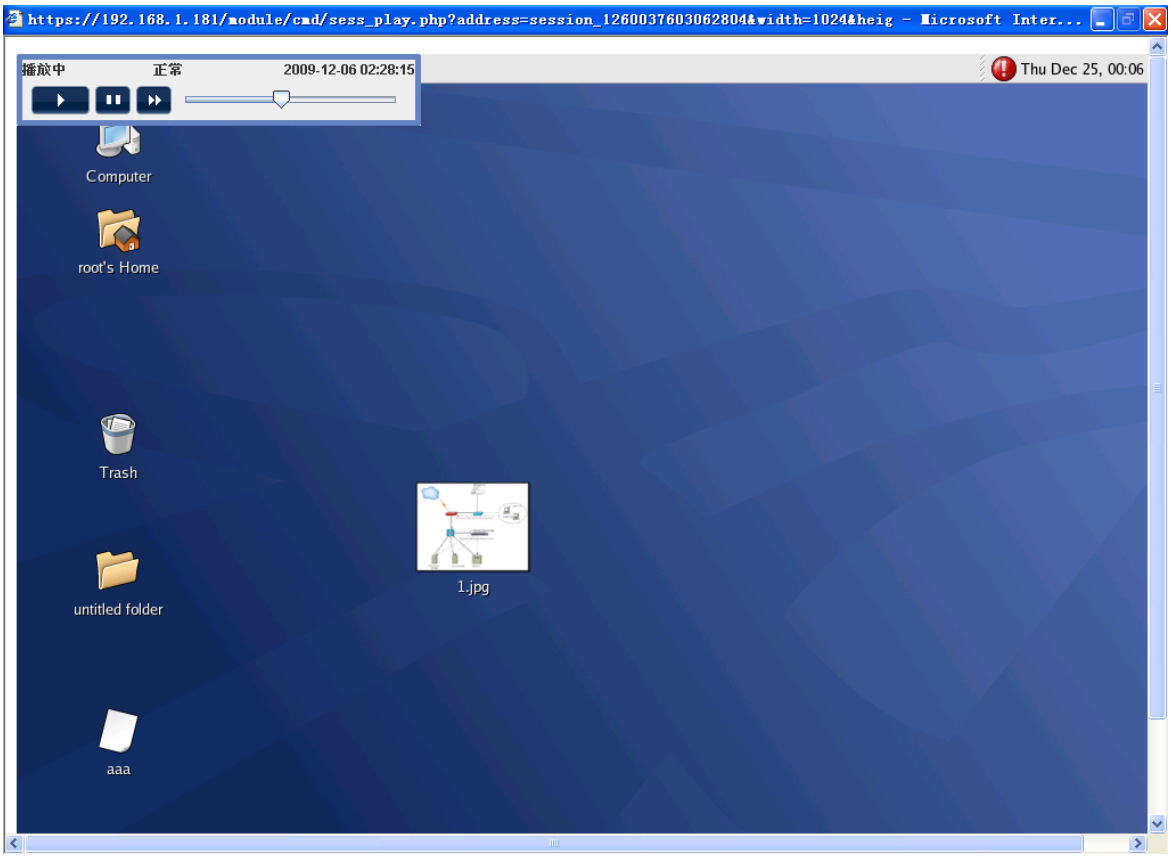


1.3 图形终端审计

针对 WINDOWS、X-WINDOW、VNC 图形界面操作审计。通过对用户的操作数据流进行实时捕获，将审计到的数据包进行逻辑重组，恢复和还原用户的远程桌面访问过程，自动以 Session 方式记录。日志查询功能提供强大的搜索引擎，实现对时间、登陆地址、主机地址、主机帐号等多种丰富的查询条件，用户可以按照自己的需要查找所关心的符合监控规则的 Session 日志。如下图：



RDP 日志回放界面



X-Window 日志回放界面

1.4 改密日志审计

显示所有网关用户密码改密情况，详情具体到某一用户密码被谁（网关用户）在什么时间什么机器 ip 上更改，参见下图：

1.5 事件日志审计

对于所有登录 UNIX 主机资产服务器后进行匹配命令控制测略操作的信息进行记录，记录信息包括系统用户、主机用户、事件时间、登录地址、主机地址、等级和具体事件。见下图：

1.6 登录日志审计

登录日志审计记录某人（网关用户）在什么时间从哪里来（登录 ip）到哪里去(目标主机)使用什么主机账号以及登录类型、登录结果和操作过什么命令。

1.7 配置日志审计

配置日志审计记录某人（网关用户）在什么时间对什么模块进行过什么配置操作，参见下图

1.8 查看详情

查看某记录详情须将鼠标移动到该记录“详情”链接上，见下图：

1.9 日志情况总揽

日志情况总揽对所有日志进行分类统计，见下图：

1.10 综合日志报表

综合日志报表为用户提供自选关键字生成报表，关键字类型包含时间范围、用户地址、用户账号、目标主机、主机账号和日志类型。报表生成支持倒序与正序方式。

点击“生成报表”按钮，生成报表详情参见下图：

您现在的位置：命令审计管理 >> 综合日志报表

2010-02-26至2010-02-26综合日志报表 [打印]

搜索条件-显示所有

类型-字符终端日志, 图形终端日志, SFTP传输日志

字符终端日志：

用户地址	用户账号	目标主机	主机帐号	时间
192.168.1.80	superman	192.168.1.143	root	2010-02-26 17:35:18
192.168.1.80	superman	192.168.1.143	root	2010-02-26 17:36:49
192.168.1.80	superman	192.168.1.61	root	2010-02-26 17:37:51
192.168.1.80	superman	192.168.1.61	root	2010-02-26 17:39:05
192.168.1.80	superman	192.168.1.143	root	2010-02-26 17:39:24

图形终端日志：

用户地址	用户账号	目标主机	主机帐号	时间

2 安全策略特性

安全策略管理是本系统的核心，它包括了统一安全管理与综合审计系统所有策略例如密码策略、账号策略以及命令控制策略等等。

2.1. 热备配置管理

正常情况下主机处于工作状态，备机处于监控状态，主备之间监控使用“心跳线”和“参考地址”方式实现。当主机出现故障时，备机主动接管主机的工作并自动升级为主机身份。故障主机恢复正常后处于备机状态，不提供服务，只负责监控实际主机的状态。当主机再次发生故障，备机同样主动接管主机的所有工作，保证服务的不间断运行，实现高可用性。

双机热备配置如下：

选中“启用热备管理”选择主机或者备机，点击“启用”按钮。

在心跳接口填入对端（备机）的心跳地址 10.1.1.2。工作接口填入对外的虚拟地址 192.168.1.199(注意：2 两个设备要设置一样的对外服务地址)，参考地址填入第 3 方存活着的主机(经常设置为网关)192.168.1.254

2.2. 组别配置管理

组别是统一安全管理与综合审计系统进行主机资产运维管理的核心，所有逻辑映射关系都建立组别基础之上，自然人、组别、主机资产、主机账号逻辑关系的建立通过权限组别管理配置实现；网关用户对应自然人，自然人可以属于一个组也可以属于多个组；主机 ip 与账号一样可以属于一个组或多个组。组别设置见下图：

2.3. 集群配置管理

集群是双机热备的一种进阶型部署，能更好的提高系统稳定性。集群部署能很好的支持跨区域部署。集群管理能更好的对整个网络进行统一管理。

集群运行模式：

单独运行模式：系统既有单独的管理配置和审计功能模块

集群中心模式：集群中心除了具有单独运行的功能，还具有调度管理节点的功能。节点上的管理配置由集群中心下发。

2.4. 应用中心设置

实现针对 SQLPLUS、TOAD、PL/SQL、KVM OVER IP、HTTP、HTTPS 等各种 C/S、B/S 应用终端的单点登录和操作的集中审计。

2.5. 系统公告设置

系统公告设置界面的公告用来提示登录 SecureCRT 用户操作信息

2.6. 网关密码策略

网关密码策略模块通过有效设置密码安全策略选项达到保护登录统一安全管理与综合审计系统密码安全的目的，策略选项包含密码最小长度、自动密码长度、密码强度选项

（包含数字、包含大写字母、包含小写字母、包含特殊字符）、密码有效期、重试锁定次数。超级用户 superman 密码被锁定后用户可以通过提供有效证件号(默认 123456)和密码（默认

superman）来取回 superman 登录密码。

2.7. 账号改密计划

帐号改密计划包含两部分：改密计划定义和应用计划对象设置。

改密计划定义包含计划名称设置，周期更新时间，强制更新时间，手工设置更新密码，密码长度与强度要求，密码保存结果给予密码管理员；可以定义多个改密计划对设备分时间段修改密码。

应用计划对象设置：设置应用计划的组别目标设备和主机帐号，参见下图：

2.8. 网关用户管理

网关用户管理模块用来添加和编辑登录统一安全管理与综合审计系统的用户相关资料

从上图显示信息我们可以得知目前统一安全管理与综合审计系统拥有 5 类用户（超级管理员、资产管理员、密码管理员、审计管理员和普通用户），用户状态皆为激活，超级管理员具有所有配置操作和审计权限没有主机帐号密码导出权限；资产管理员能添加主机资产与主机帐号，对超级管理员分配给自己的主机进行运维操作和查看自己的操作日志；密码管理员能够导出所有主机帐号密码，运维与审计超级管理员分给自己的主机；审计管理员对超级管理员分配给自己的主机进行运维操作和查看所有操作日志；普通用户只有操作超级管理员分配给自己的主机权限不能进行其它任何操作包含不能查看自己操作日志。在这张图中超级用户 superman 可以编辑任何一个用户的信息和删除除了它本身的其它用户信息。点击用户名 superman 所在记录右边的“编辑”按钮，显示画面见下图：

上图包含信息有：用户名称 superman、用户邮箱（用来接收 superman 用户密码邮件）、用户类型（超级用户）、用户状态为活动（表示此用户能够成功登录统一安全管理与综合审计系统）、密码管理选项（备注：可以自己按照密码策略要求设置密码或点击“自动密码”按钮生成复杂密码）等等。点击“个人信息”按钮进入 superman 个人资料编辑窗口：

注意：为了增强网关用户密码附件安全性统一安全管理与综合审计系统提供用户设置附件解压密码的功能，得到附件的人在不知道附件解压密码的情况下是不能继续查看附件内容的，一定程度上增强了统一安全管理与综合审计系统自身安全性。

网关用户密码可以自定义密码批量修改，点击“批量修改”，在弹出页面“批量修改密码”中输入新密码选中需要改密的网关用户最后点击“确定”按钮，批量改密成功。参见下

图：

网关用户管理界面实现了升序、降序与分页功能，页面显示记录条数由用户自定义。

2.9. 主机资产管理

主机资产管理模块用来添加、编辑和删除主机资产，该权限只有超级用户和资产管理员具备

各种类型登录方式主机资产添加举例：

使用 SSH 登录管理网络设备 Cisco 交换机添加

使用 rdp 管理 Windows xp 添加

使用 SSH 登录管理 linux 主机添加

ftp 服务器添加

主机资产管理页面支持页面记录关键字“操作系统过滤”过滤，参见下图：

为了使用户快速编辑某主机资产信息，统一安全与综合审计系统提供 ip 搜索定位功能。

2.10. 主机账号管理

主机账号管理模块用来添加、编辑和删除资产服务器账号与密码信息，并可将服务器的登录帐号赋予所属组别，账号涉及两方面的内容：

1、账号密码代填，通过统一综合管理与综合审计系统代填主机帐号和密码。

2、帐号密码同步，根据用户自定义帐号改密计划自动更新主机帐号密码。

账号密码更新设置包含三步：（1）时间同步服务器的设置（账号更新的时间参照物）（2）帐号改密计划设置与应用该计划的设备账号设置；（3）密码同步启用。

帐号分为三类：一般账号（登录目标服务器真实帐号），密码为真实帐号密码；空账号 null(适用于无帐号系统比如 VNC 或只有密码的系统登录)，密码为真实密码；unused 帐号适用于用户自己输入帐号与密码场合（设置该帐号在登录目标主机时候需要用户提供真实用户名与密码，没有密码代填功能），unused 密码不是真实帐号密码可随便填。 主机记录中字段失步的值用来代表帐号密码同步状态成功与否，失步状态为“0”代表账号密码同步，失步状态为“1”代表账号密码不同步。

2.11. 权限组别管理

权限组别管理模块负责管理系统用户、主机 ip、主机帐号逻辑关系和权限分配

a) 网关用户所属组别划分，参见下图

b) 主机 ip 所属组别划分如下图

c) **主机账号所属组别划分见下图**

2.12. 扩展命令管理

华为统一运维接入与安全审计平台支持自定义编辑批量命令集。批量命令可在多种字符系统下应用，设置好命令前缀，编辑用户所需要的命令集，支持命令排序更改，支持命令加密，支持多批量命令应用。如下图：

点击“编辑”超级连接后点击“添加”按钮。如下图：

根据实际情况添加命令集，如下图：

2.13. 扩展命令设置

在编辑命令集后，设置具体对应用户管理的主机账号执行批量命令集。如下图：

比如设置网关账号 audit 在主机 192.168.1.143 上使用账号 root 执行命令集 extand，请点击网关用户 audit 主机资产 192.168.1.143 主机账号 root 对应行的“选择”超级连接，如下图：

2.14. 命令分组管理

“命令分组管理”配合“命令控制策略”实现对用户操作高危命令的控制在该页面中用户可以添加、修改、删除命令组别。在“命令组别”后的文本框中键入命令组别名称。点击“添加”按钮，完成命令组别的添加，下图所示命令分组管理界面：

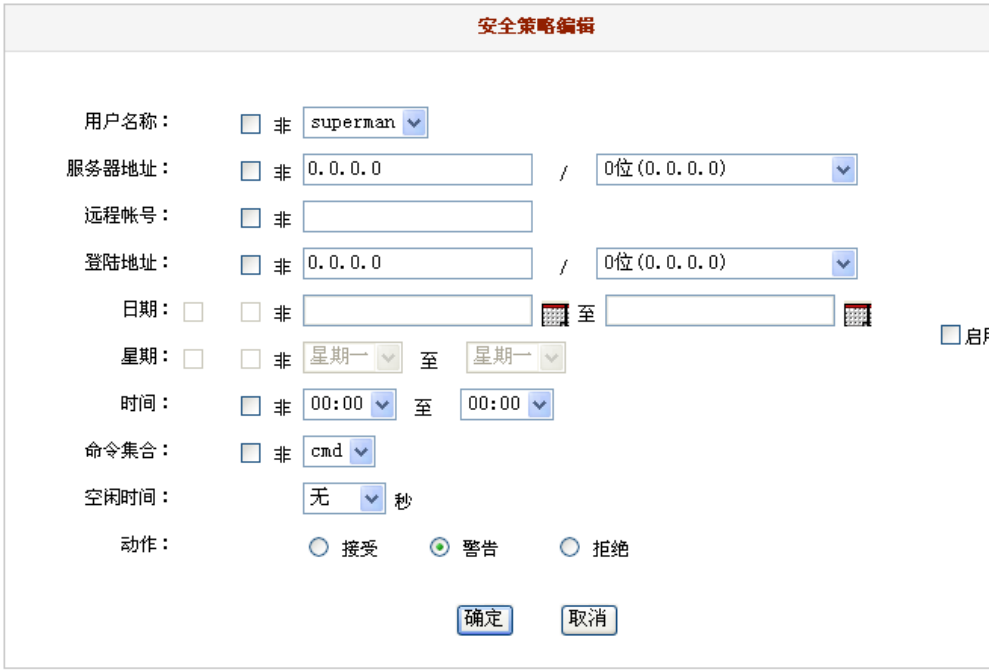
要对命令组别中的命令进行编辑操作单击“编辑”按钮，进入命令编辑菜单，如下图：

用户按命令模式（精确匹配）或参数模式（模糊匹配）在相应的文本框键入命令，单击“添加”完成该命令组别新命令添加。

2.15. 命令控制策略

策略的配置管理，用户可以根据日期、星期、时间、命令集等条件对 UNIX 主机设置安全策略。如下图：

在上图中单击“添加”按钮，进入“安全策略编辑页面”。如下图：



添加如下内容的一条策略： 用户名称（即登陆到统一安全管理与综合审计系统的用户名）superman;服务器地址（主机资产服务器地址）为 192.168.1.143/32, 远程账号（即登陆主机资产服务器 192.168.1.143 的账号）root。登陆地址为 192.168.1.80/32;日期为 2010/01/15—2010/03/31；时间为 00:00—20:00；命令集为!（非）CMD；动作接受。符合以上所有条件的用户被允许登陆主机资产服务器 192.168.1.143，执行除了 CMD 命令集中的其他命令。被成功添加的策略记录如下图：

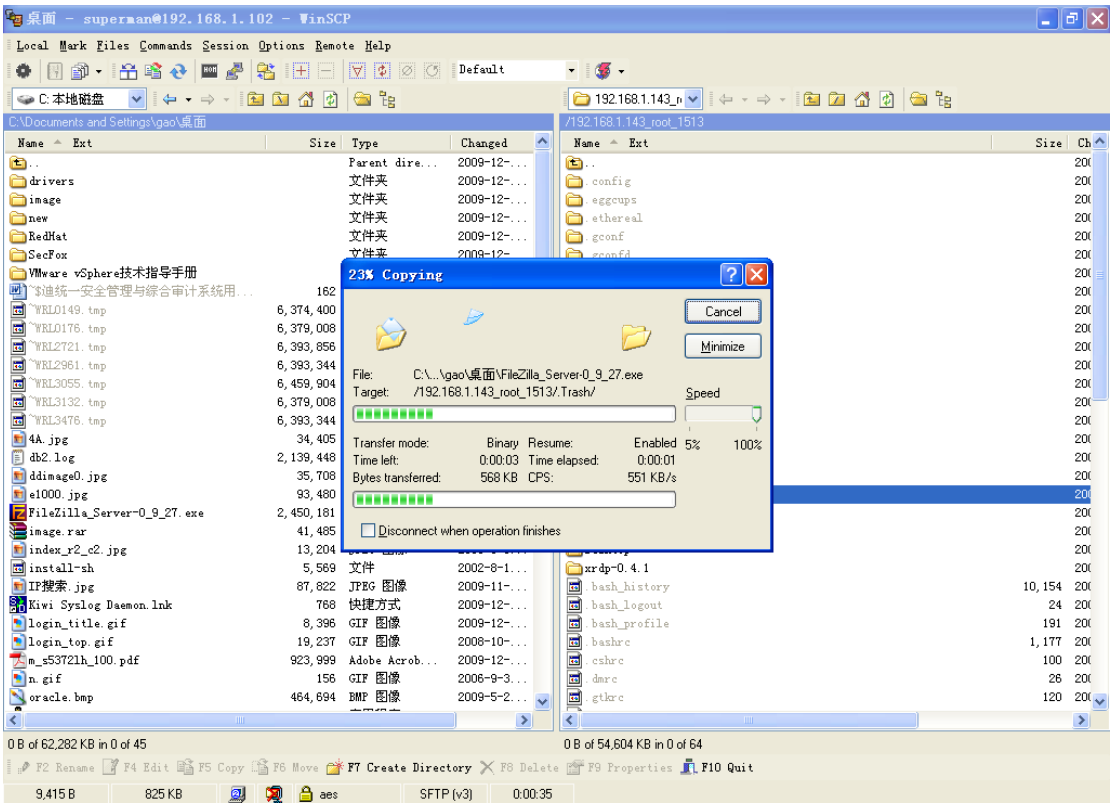
“安全策略编辑”中的日期/星期、时间、命令集合、空闲时间、动作（接受、拒绝和警告）是进行 UNIX 主机安全策略匹配的条件因子，全部条件都增加“非”的功能，完善了策略配置的灵活性和多样性。用户可以根据本地的网络情况，科学配置。

2.16. SFTP 传输管理

为方便服务器的维护和数据安全传输，推出两种文件传输方式，分别支持 FTP、SFTP 两种数据传输工具，支持任何基于上述两种协议的现有工具。针对 SFTP 协议，提出一站式传输理念，用户直接将文件通过统一安全管理与综合审计系统，将文件 SFTP 到目标主机，中间没有停留，直接到站，与此同时，整个使用 FTP， SFTP 方式传输文件的过程，都会被平台实时完整的记录下来，方便后期集中审计，责任鉴定。

点击该记录最右边“winscp 应用程序”图标进行 sftp 文件传输。

Sftp 文件传输参见下图：



3 基本特性

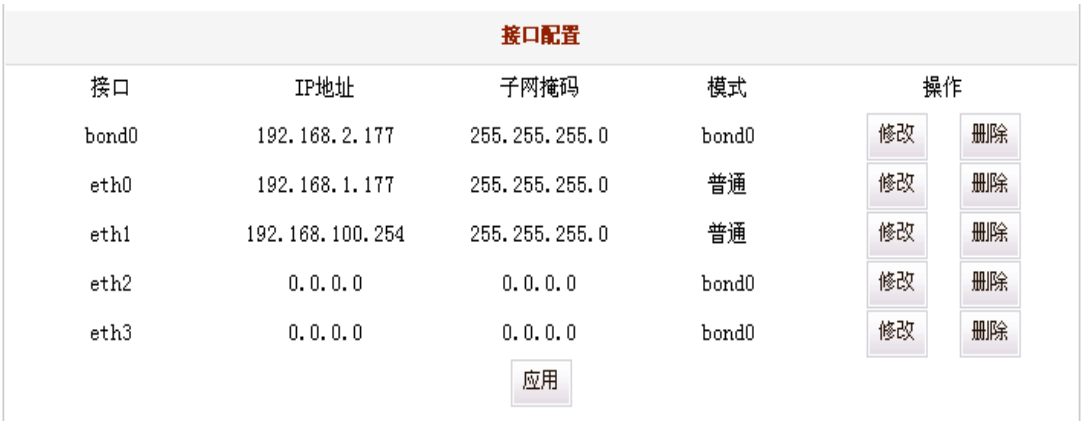
华为统一运维接入与安全审计平台的系统基本设置是对平台设备的基本参数设置，使其能够正常工作。具体包括：“系统基本配置”、“基本输出设置”、“时间同步设置”、“邮件服务设置”、“安全证书管理”、“软件注册管理”、“配置备份管理”、“RADIUS 认证”、“软件升级管理”、“设备重启停止”等选项。用鼠标单击页面左边菜单栏的“系统基本配置”菜单可以看到它所包含的子菜单项，界面如左图所示。

3.1 系统基本配置

华为统一运维接入与安全审计平台的系统基本配置包括对平台设备的网卡及相

关参数的设置。界面如下图所示：

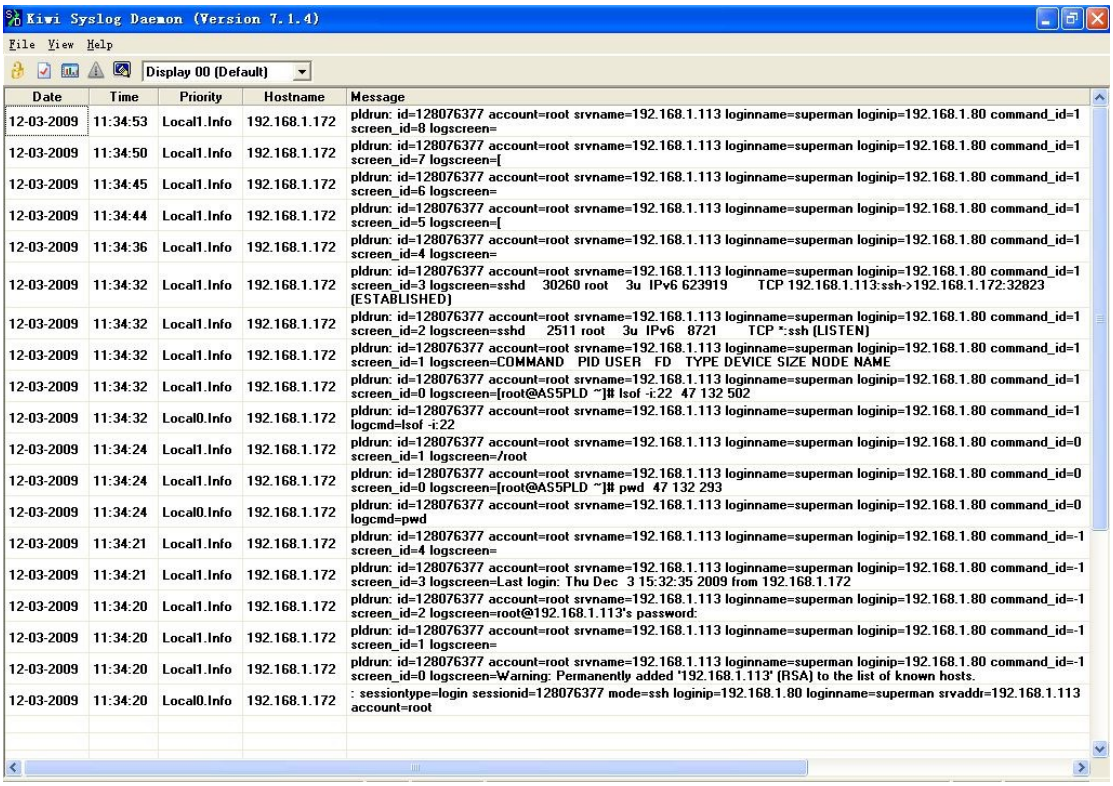
管理员可以根据实际网络情况，合理配置网络参数。管理员对网络参数的设置，无需设备重启或服务重启，将会立即生效。华为统一运维接入与安全审计平台的网卡属性拥有普通和 Bond 两种模式。普通模式即网卡的正常模式；Bond 模式用两块网卡来提供网卡冗余功能，工作方式是主备的工作方式,也就是说默认情况下只有一块网卡工作,另一块做备份。界面如下图所示：



3.2 基本输出设置

对 SYSLOG 日志服务器（一般安装在个人 Windows PC 上）参数设置：包括日志服务器地址和“启动/停止”设置，将日志输出到 syslog 服务器展现，设置见下图：

日志效果参见下图：

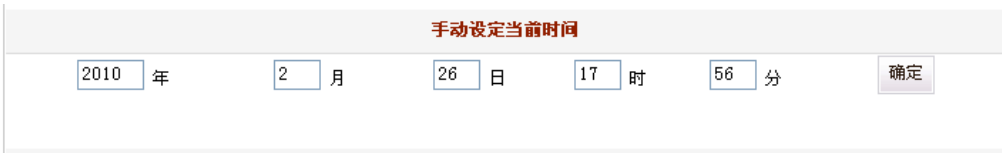


3.3 时间同步设置

华为统一运维接入与安全审计平台的策略控制提供日期/时间控制的策略因子。所以日期/时间的准确性相当重要，而华为统一运维接入与安全审计平台提供的时间同步功能能够与世界标准

时间相一致，保证了策略控制的准确性。但使用时间同步功能的同时必须保证平台系统能和 Internet 网络相连通。界面如下图所示：

华为统一运维接入与安全审计平台的时间设置功能，不但能够与国际标准时间相同步，管理员还可以根据实际环境设置时间/日期。如下图所示：



3.4 邮件服务设置

为密码安全着想和日后用户忘记登录统一安全管理与综合审计系统密码，统一安全管理与综合审计系统提供方法：把用户登录统一安全管理与综合审计系统的密码在系统用户注册或编辑的时候通过发送邮件发给用户预先设置的邮箱。

点击“系统配置管理”中的“邮件服务设置”菜单项，进入“邮件服务设置”页面

为了发送网关用户密码邮件须设置统一安全管理与综合审计系统网关地址与 DNS 信息（确保网络畅通）和发送邮箱信息，统一安全管理与综合审计系统支持邮件传输方式有：普通传输和 SSL 加密传输（支持 SSL 加密传输邮件需发送邮箱与接受邮箱同时支持加密功能（例如：GMAIL 邮箱）。

3.5 安全证书管理

为了增强代管主机帐号密码安全性统一安全管理与综合审计系统采用认证证书加密密码文件，密码管理员使用帐号导出功能下载主机帐号密码文件只有借助加密证书和解密工具才能解密主机帐号密码文件获得最终帐号密码信息。安全证书管理提供超级管理员生成加密证书与下载功能，输入证书密码参见下图：

点击 “生成证书”按钮，证书生成（只有超级用户拥有生成证书权限）

超级用户和密码管理员可以下载证书；超级用户虽然不能导出密码加密文件但是它拥有清除证书权限。

3.6 软件注册管理

每台华为统一运维接入与安全审计平台都有一个唯一的序列号，当系统升级或其他原因要重新安装系统时，则必须要输入这个唯一的序列号。

每台华为统一运维接入与安全审计平台的序列号都是唯一的，不能重用，这样有效的保护了华为统一运维接入与安全审计平台的版权，也给市场有续的运营提供安全保障。如下图：

3.7 配置备份管理

配置备份管理备份已有配置信息，包含组别信息、网关用户信息、主机资产信息、主机账号信息等等，支持备份文件下载到本地。

3.8 RADIUS 认证

平台支持标准的 Radius 认证协议，能够很方便的和身份认证产品集成，提升产品安全性和扩展性,如下图：

在端口信息填入 RADIUS 的 IP 和端口号，私钥密码为 RADIUS 的私钥，点击“确定”完成配置；将平台以认证客户端添加进 Radius 服务器；在平台的 WEB 控制台添加网关用户即主账号（对应自然人），网关用户必须在 RADIUS 认证服务器上真实存在，且网关用户与令牌 ID 相关联（如果未关联那么平台网关用户即令牌 ID）。

3.9 软件升级管理

软件升级菜单用于对华为统一运维接入与安全审计平台的功能进行升级。单击菜单栏上“软件升级管理”可进入软件升级页面。

软件升级有两种方式，软件包上载升级为系统管理员通过将本地的软件升级包上载到华为统一运维接入与安全审计平台进而实现系统升级的一种软件升级方式。

指定服务器升级为系统管理员从一个给定的服务器下载指定文件来进行华为统一运维接入与安全审计平台软件升级的一种软件升级方式。输入升级服务器的地址和升级文件的文件名，单击“确定”，如果升级包格式错误或者升级包加密验证错误，将提示错误验证信息。

3.10 设备重启停止

“设备重启停止”用来重启设备和关闭设备