运维安全堡垒平台管理员手册

中远麒麟产品部

目录

1 概述

iAudit 运维安全堡垒平台（以下简称 iAudit 运维堡垒机）是用于对第三方或者内部运维管理员的运维操作行为进行集中管控审计的系统。iAudit 运维堡垒机可以帮助客户规范运维操作行为、控制并降低安全风险、满足等级保护级其他法规对 IT 内控合规性的要求。

1.1 功能介绍

iAudit 运维堡垒机集中管理运维账号、资产设备，集中控制运维操作行为，能够实现实时监控、阻断、告警，以及事后的审计与统计分析。

iAudit 支持常用的运维工具协议（如 SSH、telnet、ftp、sftp、RDP、VNC 等），并可以应用发布的方式支持图形化运维工具。

iAudit 运维堡垒机支持旁路模式和 VPN 模式两种方式，物理上旁路部署，灵活方面。

iAudit 运维堡垒机在操作方式上，不改变用户的操作习惯，仍然可以使用自己本机的运维工具。

1.2 名词解释

控制台

指 iAudit 运维堡垒机提供给管理员实现对它进行管理的 Web 系统。

管理员

指 iAudit 运维堡垒机系统的管理员，按照角色分为系超级管理员、配置管理员、组管理员、密码管理员、审计员，按照权限分立的原则分别承担不同的职责。

超级管理员：是内置的最高权限管理员，可以创建其他管理员角色用户账号。

配置管理员：负责资产管理、授权管理等。

组管理员：只对特定组的资产管理、授权管理。

审计员：只负责完成审计工作；

密码管理员：负责维护资产设备的账号密码。

协议

指 iAudit 运维堡垒机运维工具所用的通信协议，比如 Putty 使用 SSH 协议，CRT 支持 SSH 和 Telnet 等。

工具

指运维人员实现对设备的维护所使用的工具软件。

设备账号

指运维目标资产设备的用于维护的系统账户。

自动登录

指 iAudit 运维堡垒机为运维工具实现自动登录目标被管设备，而运维用户不需要输入目标设备的登录账号和密码，也称为单点登录（SSO）。

命令阻断

指 iAudit 根据命令权限策略检查用户输入的操作指令，如果策略不允许执行此指令，iAudit 会拒绝转发此操作命令目标设备，同时向操作员反馈拒绝执行的提示信息。这是实现实时操作控制的一种重要手段。

应用发布

指通过在应用发布服务器部署应用程序，提供给用户远程虚拟化方式进行使用，就如同安装在本地一样的效果。

1.3 环境要求

iAudit 运维堡垒机管理控制台为 Web 系统，要求客户端采用支持 IE 内核的浏览器登录，因为需要支持 ActiveX 控件，推荐使用 IE 浏览器，支持 IE8、IE9、IE10。。另外，终端还需要安装 JRE 环境，支持 iAudit Web Portal 的 Java Applet。

2 管理员登录

iAudit 运维堡垒机管理控制台采用 HTTPS 安全通信连接，默认端口是 443。管理员登录控制台的方式是，以 IE 为例，在浏览器地址栏输入：

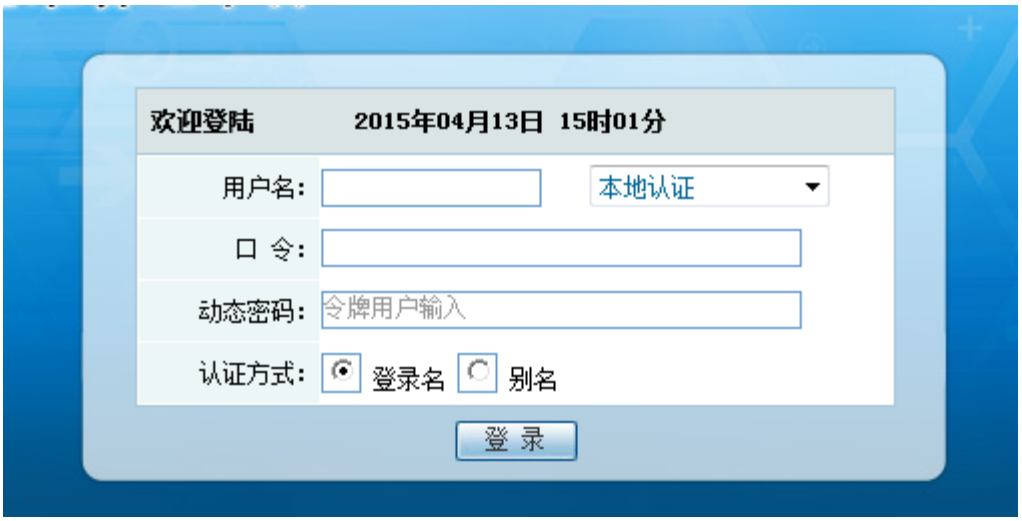
https://iAudit-ip

iAudit 运维堡垒机超级管理员的账号和密码是“admin/12345678”。

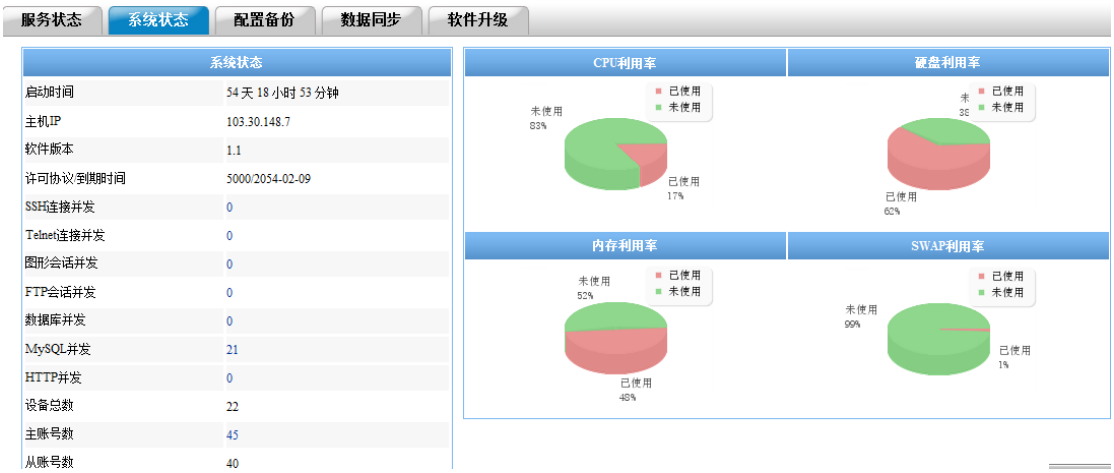
iAudit 运维堡垒机初始状态未启用动态口令认证，因此初次登录不需要输入动态口令。

另外，iAudit 运维堡垒机还有两个预设的管理员用户，audit 和 password，分别是审计员账户和密码管理员账户，默认密码也是“12345678”。

管理控制台登录界面如下图所示。



登录成功后界面如下图，进入系统当前状态界面。然后管理员可以根据需要选择功能菜单执行预期的管理操作。



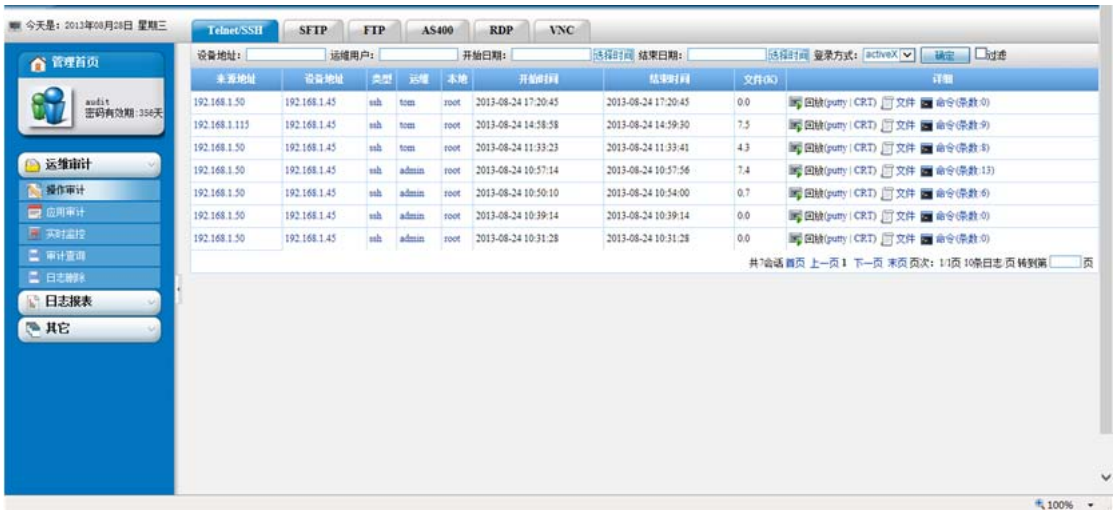
超级管理员可以完成其他所有管理员可以做的工作，因此超级管理员界面的功能就是管理控制台的所有功能，其他管理员操作界面只是其的一个子集。

以非超级管理员的其他管理员身份登录，系统会要求首先修改个人账户密码，如下图所示：

配置管理员登录后的操作界面如下图所示：

密码管理员登录后的操作界面如下图所示：

审计员登录后的操作界面如下图所示：



组管理登录后的操作界面如下图所示：

不同角色管理员功能职责允许有交叉，超级管理员可以承担所有管理工作，比如他可以承担审计员的工作，其他管理员权限也可以根据需要进行授权。本文档对管理员功能的介绍按照功能模块进行组织，不同角色管理员根据自己的授权和管理界面，在对应功能模块章节查看操作说明。

3 初始基本配置

开始使用堡垒机，管理员应先进行一下配置检查，根据实际应用需要配置必要的系统参数，构建适合本单位的系统工作环境。

1、 系统时间同步

系统配置—参数配置中的系统参数选项卡中各项需要确认，尤其是系统时间，有条件的请配置合适的 NTP 服务器，保证运维堡垒机时间的准确性。

2、密码策略

账号管理是 iAudit 运维堡垒机的核心功能之一，账号密码的安全性不容忽视，应在创建账号前首先确定密码安全策略，如下图所以。

3、资产设备系统类型

资产设备管理进行运维安全管理的基础，每台资产设备都有相应的系统类型，检查和配置系统类型是开始资产管理的基础，应在添加资产前首先配置好资产系统类型，如下图所示。

4 目录管理

4.1 目录说明

目录结构就是 LDAP 的目录 ，目录中可以放置主帐号、服务器等资产，因为系统为目录结构，因此，帐号和服务器可以放在同一个目录中，即目录与过去的

资源组不同，没有区分是用户的或是设备的，任何一个目录中即可以放置主帐号，也可以放置服务器等资产。

目录主要功能是方便管理，使用目录结构，当需要进行查找时可以直接以目录为单位进行，方便了管理人员使用。

系统上线前必须划分好目录结构，小的环境中，建议使用平装单层结构，即只有一层组，大的环境中，建议使用三级目录关系，即系统可以分为一级目录 、二级目录 和组三层。

4.2 目录创建

目录创建时，小的环境中，直接创建资源组即可，设备组与设备组之间是平等的，用户在创建主帐号或资产时，直接将主帐号或资产加入到资源组中即可。

大的环境中，用户需要先有一个规划，一般可以按地点或管理结构进行规划，系统可以设置为一级目录-二级目录-资源组三层关系，二级目录必须在一级目录中，资源组即可以在一级目录中，也可以在二级目录中，用户在资源管理-目录管理中点击新建，在节点类型中选择为一级目录，输入节点名称和描述点确认即可以建立一个一级目录 。

建立一级目录 后，用户可以在点击新建按钮，创建二级目录或资源组，并

且将新建的目录或级加到刚才的一级目录中。

建立好目录关系后，在目录管理中，可以直接查看目录与资源组之间的关系

5 账号管理

5.1 用户角色

iAudit 运维堡垒机设置了五个用户角色：超级管理员、配置管理员、审计管理员、密码保管员和普通用户，各角色具体权限如下表所示。

用户角色	角色权限
超级管理员	账户管理 资产管理 系统级配置管理 运维审计策略配置 运维操作审计
配置管理员	资产管理 运维操作审计
分组管理员	资产管理：角色类似配置管理员，但是只能对指定设备组进行管理 运维操作审计
审计管理员	运维操作审计 运维审计报表
密码管理员	密码管理
普通用户	设备运维

iAudit 出厂内置三个管理员账户，分别是：

（1） admin —超级管理员

（2） audit ——审计管理员

（3） password ——密码管理员

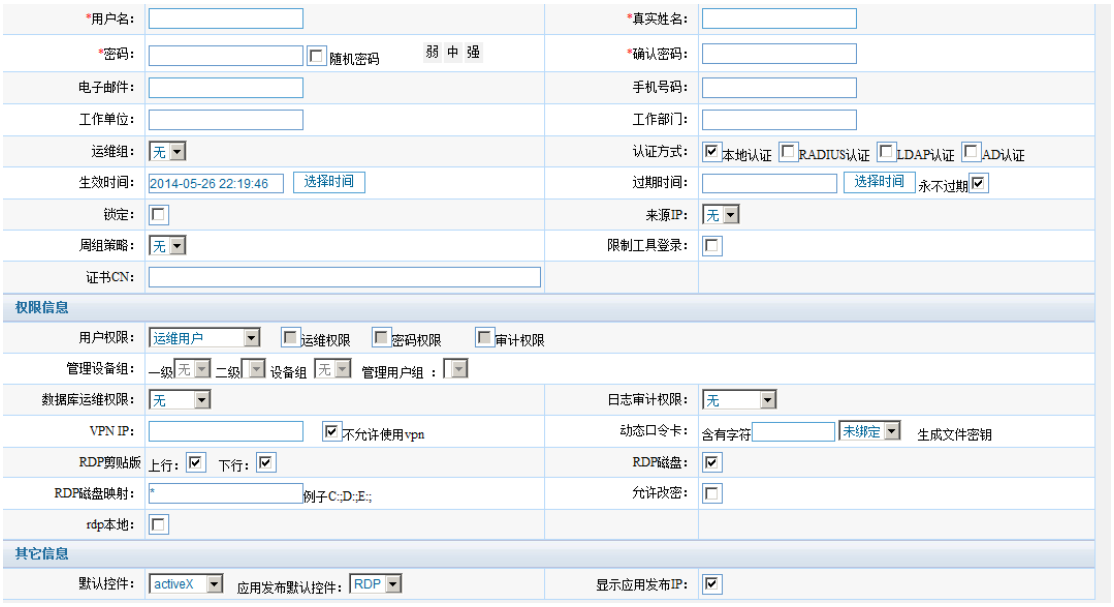
三个默认用户的默认密码均为 12345678。

5.2 运维账号管理

点击左侧菜单“资源管理—运维账号”，打开运维账号管理界面。初始界面可以看到三个管理员账号。

在运维账号列表底下有一排操作按钮，用来实现账号相关的管理工作。

5.2.1 添加用户



每个运维账号含有大量权限信息，是理解运维控制的核心，请务必仔细领会，下面详细介绍。

1、 账户基本信息

账户基本信息主要包括账户的基本

标识信息、对应自然人信息、有效期和账户认证相关信息。

用户组：是为了方便分组管理设置的组，可在同一界面的“目录管理”选项卡中设置用户组，注意，用户在添加时，必须属于一个组。

认证方式：本地认证、外部认证、短信认证。默认采用本地认证，如果使用 Radius 账号，用户认证方式就是外部认证方式。另外，动态口令方式认证也属于外部认证。

生效时间：账号启用的时间。

过期时间：设定账号有效期。有一定使用时间期限的账户也称为临时账户。

锁　　定：是使该账号暂时不可用，解锁后可以正常使用。

来 源 IP：设定给用户的来源 IP。来源 IP 的具体 IP 列表设定在“资源管理—策略设置”界面中。

周组策略：设定该账号一周七天中，哪些天和每天什么时段可以有效访问。

限制工具登录：限制用户使用工具登录。

2、 权限信息

用户权限：本行设定用户角色和其操作权限。从下拉列表框中选择用户角色，该账号即有了角色的默认基本权限；下拉框本行右侧的各选项，是角色基本权限外可扩展的权限，如果可选表示角色可以赋予该权限，如果不可选表示不能赋予该权限。角色可扩展权限如下图所示。

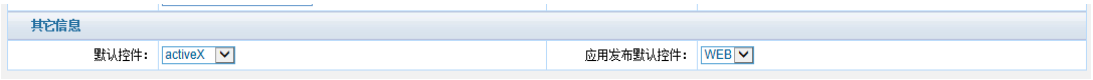
角色	可扩展权限
普通用户	无
管理员	运维权限、密码权限
审计员	运维权限、密码权限
密码管理员	运维权限
配置管理员	运维权限、密码权限、审计权限
组管理员	运维权限、密码权限、设备组、用户组

数据库运维权限：该账户运维数据局库的时候是数据库 DBA 还是普通用户等权限登录。

日志审计权限：日志审计功能的权限设置。

VPN IP：勾选“不允许使用 VPN”，表示不能以 VPN 方式登录堡垒机。如果不打勾，表示允许该账户通过启动堡垒机的 VPN 客户端登录堡垒机进行运维。VPN IP 一般不用指定，堡垒机会自动分配 VPN IP。

3、 其他信息



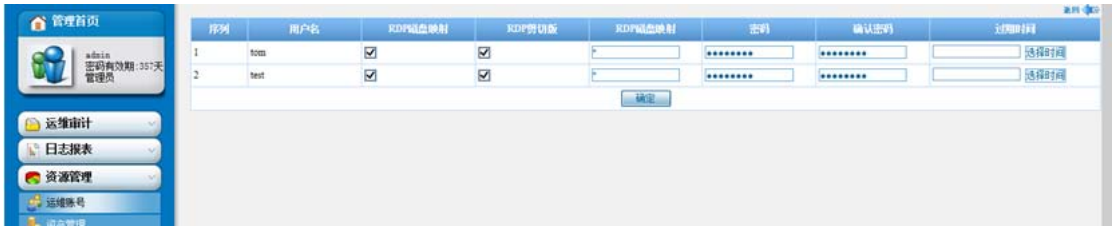
设置用户使用控件的方式。

5.2.2 批量添加用户

点击“批量添加”可以快速添加多个用户，如下图所示。

5.2.3 批量编辑用户

点击“批量编辑”按钮可以快速编辑多个用户信息，如下图所示。



5.3 RADIUS 账号

“Radius 账号列表”是在采用 Radius 认证方式的时候使用的，用户管理理念和维护 Radius 账户信息，各按钮含义与前面本地用户操作相同，只是现在目标本地账号系统变成了外部的 Radius 账号服务器。

添加 Radius 用户的项目信息如下图所示：

5.4 目录管理

系统使用标准的 LDAP 树型结构，因此资产必须属于树中，比如运维人员帐号、设备资产等，必须在一个树中。

目录管理菜单可以建立或编辑树形结构，可以将资产加入相应的树形结构中，一般情况下，树形结构是按公司的组织方式进行添加。

5.5 在线用户管理

在线用户管理用于查看用户状态，并可对在线用户进行控制管理，主要是断开操作。当认为当前用户不适合继续在线操作时可以执行强制“断开”，使其下线。从在线用户列表中可以看到用户的登录时间和来源 IP。

5.6 登录策略

绑定授权访问策略，限定用户登录运维资产的合法时间，具体策略规则在“资产管理-策略设置-授权策略”中配置。默认是没有登录策略限制，即每天任何时

间都可以登录运维。

5.7 设备管理

“资源管理-资产管理”菜单的“设备列表”选项卡实现设备管理的功能。打开该选项卡首先看到的是当前已有设备列表，如下图所示。

有关设备的相关在添加或修改界面上能够充分体现。点击“添加新设备”打开添加设备界面，如下图。

服务器地址：必填项

主机名：必填项

设备组：可选项。设备组需要在统一界面的“设备组列表”选项卡进行设置。

系统类型：必须正确选择。如何配置系统类型列表，在“第三章 初始基本配置”中已经有介绍。

超级管理员口令：一般不需要填写，保持空白即可。一些路由交换机等设备

从普通用户登录时自动 su 到 root 时才需要填写。一般的 Windows、Linux、Unix 服务器设备不用填写此项。

修改方式：指自动修改设备账号密码的改密频率，与下一行的频率共同使用，频率底下一行是提示说明。如果不想自动改密，请填写 0。

各种协议默认端口：是指如果该设备上使用该协议的话，所使用的端口，如果实际情况不是标准默认端口，请修改成为实际端口值。

Oracle 实例：Oracle 服务器时添加服务名。

扩展信息：是一些常规资产管理信息，如果需要可以填写，一般可以不填。内容如下图所示。

对已有设备的管理最主要操作用户绑定，点击下图中设备所在行右侧操作栏中的“用户”链接。

点击“用户”链接后，打开设备的系统用户管理界面，如下图所示。

可以为当前设备添加、删除系统用户。系统用户是真正登录到该设备的最终

执行账号。

点击“添加新用户”可以看到系统账号的相关信息，如下图所示。

用户名：必填项。

空用户：对于一些特殊的设备才有用，一般是不用选此项的。

Radius 用户认证：如果设备登录涉及 Radius 认证请勾选。

登录方式：必选项，必须正确选择。在选择 ssh 登录方式的时候，如果账号同时允许 sftp，可以勾选“sftp 传输”。

端口：确认登录方式协议对应的端口。

过期时间：系统账号停止使用的时间。

用户终端：只终端输入输出字符集，一般默认即可，如果是中文界面，出现乱码的时候可以尝试选择 GB2312。

启用：勾选启用，该账号可以正常使用；如果不勾选，该账号暂时不可使用。

自动修改密码：该账号的密码是否允许自动修改。

改密主账号：该账号是否是用来修改密码的主账号。一般选择设备上具有超级管理员权限的账号作为改密主账号。

设置自动改密，还需要配置自动改密的密码测试，在“资源管理-策略设置-自动改密”选项卡中设置改密的密码策略。如下图所示。

修改密码主账号是指修改密码时 iAudit 堡垒机使用的账号，建议使用权限最高的 root 或者 administrator 来作为主账号，以免在 iAudit 系统自定义的改密规则和被管理的设备系统的默认改密规则冲突。

iAudit 堡垒机自动修改密码，其中 Unix 设备使用 telnet 远程改密，Windows 设备需要在目标服务器安装 agent。

自动登录：堡垒机为用户启账号密码代填登录。不选择自动登录，用户需要自己输入系统账号、密码。

公私鈅认证：当目标设备采用公私钥认证方式时选此项。

绑定组：设备的运维权限授予指定组。

绑定用户：设备运维权限授予指定用户。

特别注意对用户的运维访问权限设置还有一个层面，点击绑定组中的一个组名或者绑定用户中的一个用户名，会打开一个设置界面，如下图所示：

账号是否被锁定：一般不要勾选，勾选后这个系统账号将不能登录。

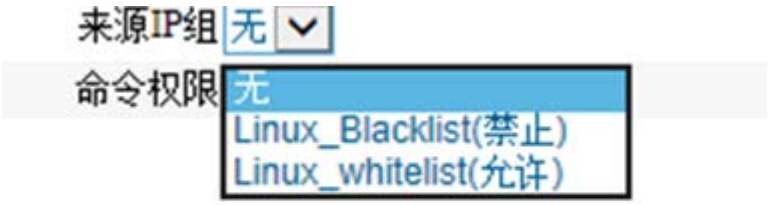
磁盘映射、剪切板对 RDP 有效。

周组策略：选择预设的周组策略。

来源 IP 组：限定运维登录的合法 IP 组。

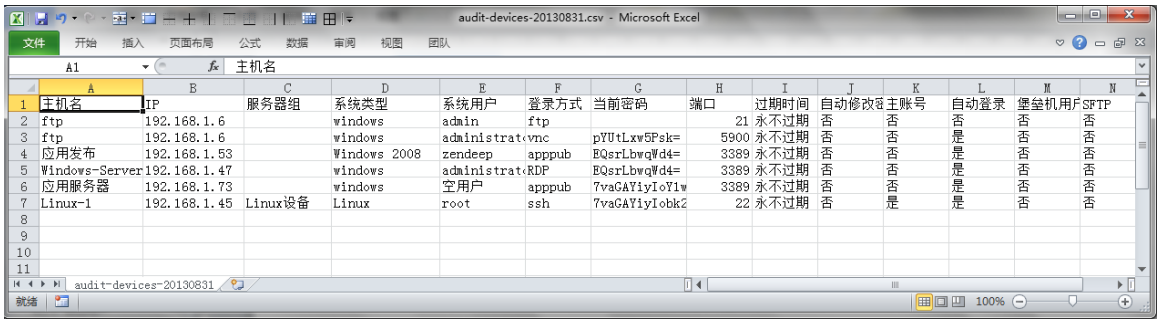
命令权限：选择预设的命令权限组。如下图所示，如果一个命令组的名称后面标有“（禁止）”表示是一个命令黑名单，标有“（允许）”说明是一个白名单。

周组策略、来源 IP 组和命令权限都说是在“资源管理—策略设置”菜单界面中。



5.8 设备信息导入导出

iAudit 运维堡垒机支持设备导入导出，采用 Excel CSV 文件格式。如下图所示。



如下图中，设备列表底下的“导入用户”、“导出用户”两个按钮就是用来导入和导出设备资产信息的，包含设备用户信息。

点击“导出用户”按钮，可以得到一个 Excel CSV 文件，可以作为模板，用

来填写需要导入的设备用户信息。

设备导入时，在资产 CSV 中添写的是明文密码，则需要将加密项勾选，系统入库时会自动将密码进行加密保存，如下图所示。

5.9 普通用户自动登录 root 账号

如果您设备不允许的root账号远程登录，需要使用从普通账号自动SU到root账号的功能。

首先在设备添加时需要输入超级管理员口令，然后将建好的普通账号绑定给指定堡垒机用户，点击堡垒机用户名进行策略设置，选择自动登录为超级用户，设置界面如下：

注意：su 切换仅对 telnet、ssh 有效，对其它协议无效

5.10 目录节点管理

点击“目录节点”选项卡，进入目录节点管理界面，如下图所示。

点击添加，可以添加设备目录节点，设备目录节点可以分为一级节点、二级节点、设备组三个级别，其中二级节点必须属于一个一级节点

在设备组目录中，点击一个目录，例如点击上图中“Windows 设备组”，系统显示出改组设备的列表，如下图所示。可以对该组设备进行操作，或者为当前组添加、删除设备

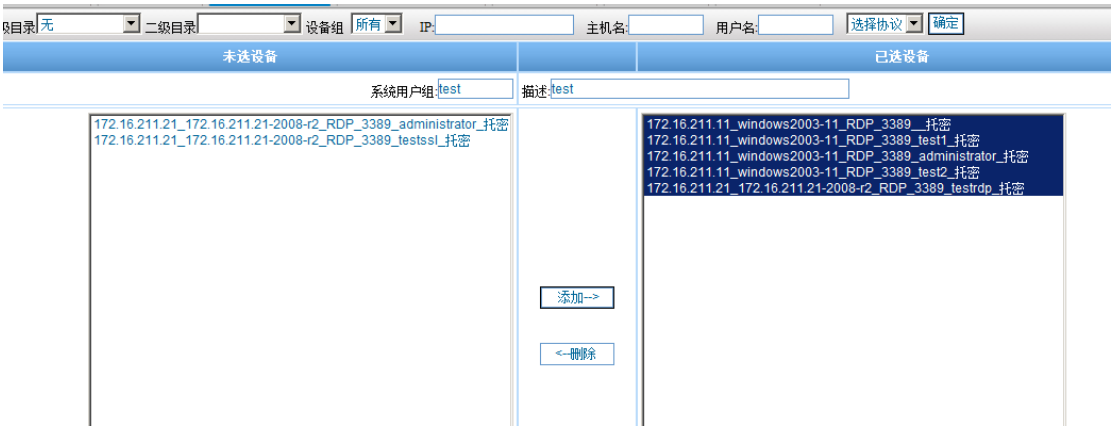
5.11 系统用户组

通过系统用户组可以快速地将多个设备的系统账号绑定给堡垒机自然人运维账号。

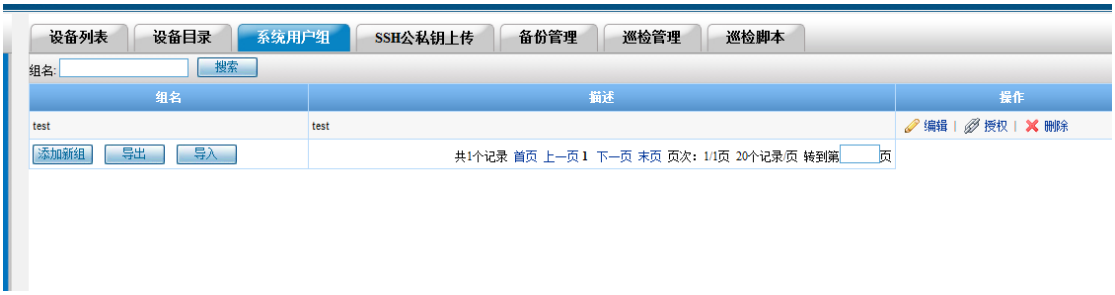
系统用户组是指将已经添加的资源的系统账号以列表的形式展现出来，方便分组绑定操作，不用再繁琐的选择资源再选择系统用户然后再进行绑定，简化绑定操作。

点击添加新组就可以添加一个新的系统用户组，界面如下：

点击“添加新组”进入新组创建页面，如下图所示。输入 IP 地址段可以对备选设备系统账号进行过滤筛选。选中要添加的账户，点击“添加”按钮，添加到组中的账号显示在右侧列表中，初始为空。



要为一个系统设备组绑定用户，请单击系统用户组列表操作栏的“授权”操作下图所示。



点击“绑定”后，进入运维账号选择绑定操作界面，如下图所示，选择需要绑定的组与用户，点击“保存修改”即可。

使用系统用户组来进行绑定可以避免系统账号绑定给自然人账号时的误操作，提供了一个更加清晰高效的绑定界面。

5.12 应用发布

应用发布系统可以管理 http/https 或 C/S 应用，比如 Juniper 防火墙，前置交换机等所使用的运维管理工具软件。

5.12.1 应用发布服务器

应用发布系统运行在 Windows 平台，推荐 Windows Server 2008，Windows 2003 也可以支持。在应用发布服务器上部署 iAudit 应用发布模块，将运维需要的各种应用程序安装在应用发布服务器上。

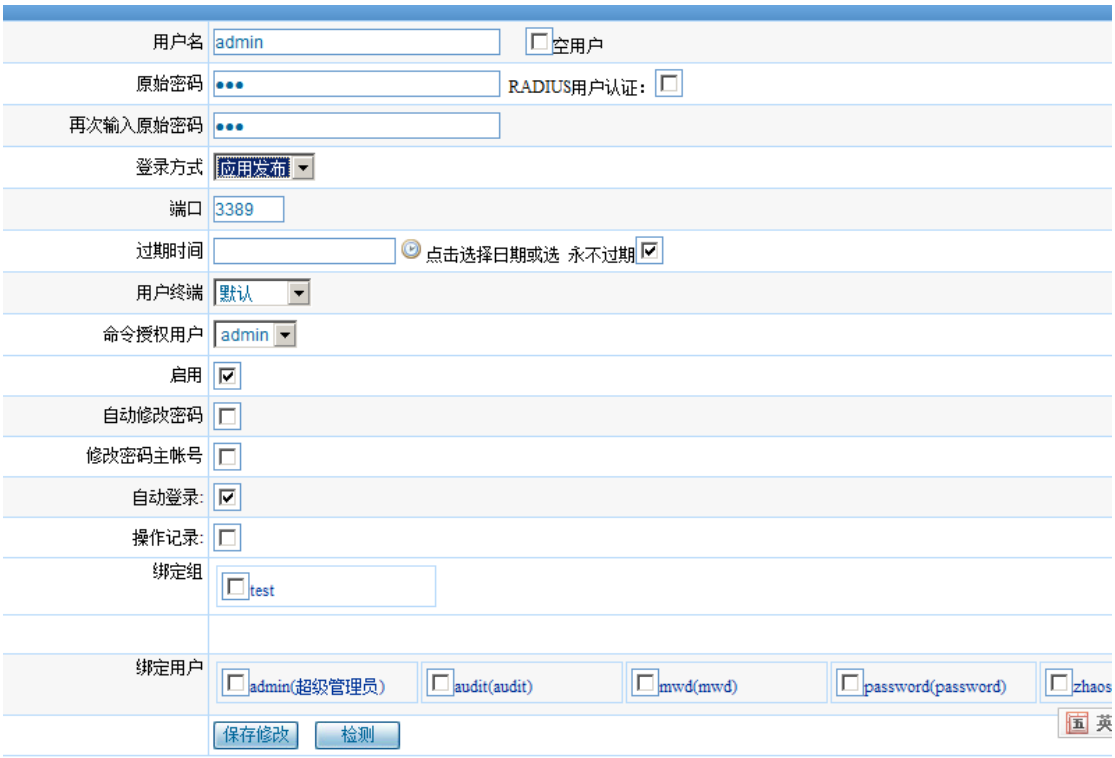
5.12.2 添加为资产设备

应用发布服务器需要先添加到系统资产里，过程与添加一台普通 Windows 服务器类似，唯一的区别是选择登陆方式为 apppud，将该设备绑定给所有需要使用应用发布的账号。

1、添加设备

2、 设置为应用发布登录模式

在设备列表中，为应用发布设备添加一个用户，用户名和密码可以为空，选择“应用发布”登录方式，保存修改。如下图所示。



5.12.3 添加为应用发布服务器

打开“资源管理-设备管理”，打开应用发布选项卡，进入应用发布服务器管理界面。可以看到应用发布服务器列表，如下图。

点击“增加”按钮，可以添加新的应用发布服务器：

5.12.4 应用发布

打开应用发布服务器列表，在操作栏中点击“应用发布”，进入应用发布界面。如下图所示显示已经发布的应用列表。

点击“添加”按钮，发布一个新的应用，注意，发布应用前，应用必须已经安装在服务器上。发布一个新应用的界面如下图所示。

应用名称：名称是唯一的，不能重复。

用户名和密码：是针对 IE 应用的，例如发布了一个邮件应用，填写邮箱的用户名和密码后可以将邮件的用户名密码自动填写。

服务器列表：选择应用在哪台服务器上。

程序列表：堡垒机系统维护的常用应用程序的列表，在当前界面的最后一个选项卡“应用程序”中可以查看和维护，如下图所示。

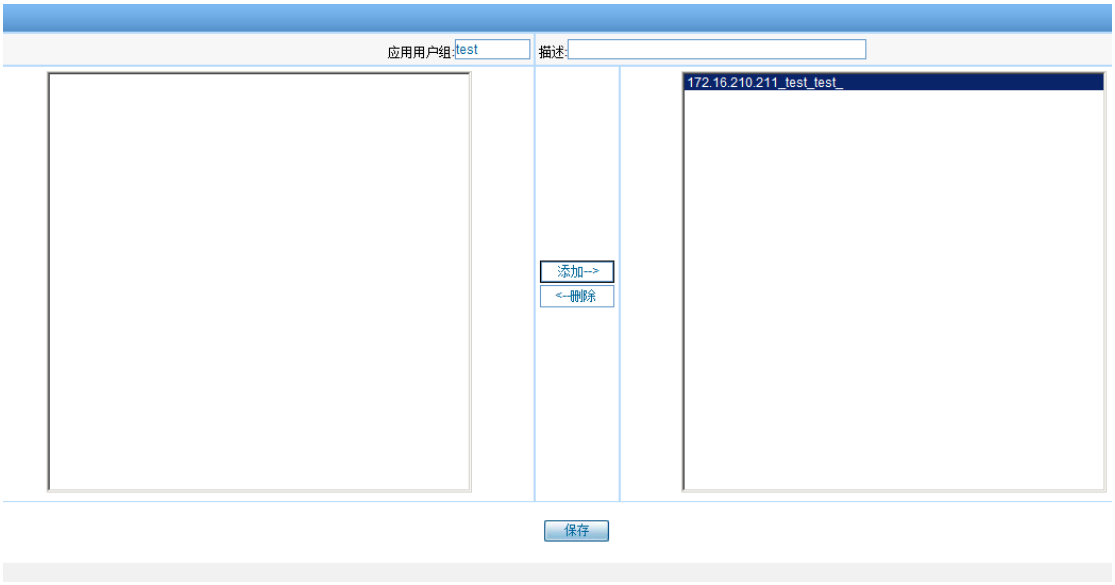
#	应用名称	程序路径	描述	操作
	cmd	c:\windows\system32\cmd.exe	cmd.exe	编辑 | 删除
	Firefox	C:\Program Files\Mozilla Firefox\firefox.exe		编辑 | 删除
	IE	C:\Program Files\Internet Explorer\iexplore.exe	test	编辑 | 删除
	IE8	C:\Program Files (x86)\Internet Explorer\iexplore.exe		编辑 | 删除
	notepad	c:\windows\system32\notepad.exe		编辑 | 删除
	Pcanywhere	C:\Program Files\Symantec\pcAnywhere\PCAQuickConnect.exe		编辑 | 删除
	PL8	E:\Program Files\plsql developer\plsqldev.exe		编辑 | 删除
	PLSQL	C:\Program Files\PLSQL Developer\plsqldev.exe	pl/sql	编辑 | 删除
	PLSQL2008	C:\Program Files (x86)\PLSQL Developer\plsqldev.exe	plsql2008	编辑 | 删除

当发布的应用是 IE 浏览器时，会在“程序地址”底下多出一行“URL”，可以通过指定 URL 对 IE 限制只能登陆指定 URL。如下图所示。

发布应用程序的授权绑定操作与设备的授权绑定完全相同。

首先在应用用户组根据需要发布的应用建立一个自定义组，再将这个应用组和用户绑定。

创建应用用户组的界面如下图所示。



下图是应用用户组绑定运维和用户和用户组的操作界面。

5.13 SSH 公私鈅上传

针对需要使用公私鈅认证的设备，上传公私鈅的界面如下图所示。

6 权限查询

“权限查询”是为了提供一种快速全面复核授权的方法，以免赋予过高的权限，或者有授权遗漏。

“权限查询”分“系统权限”和“应用权限”两大类进行查询。“系统权限”对应就是资产设备运维权限，“应用权限”就是发布的应用程序的权限查询。

在权限查询界面还可以直接链接到授权绑定的修改界面，便于快速修改授权。

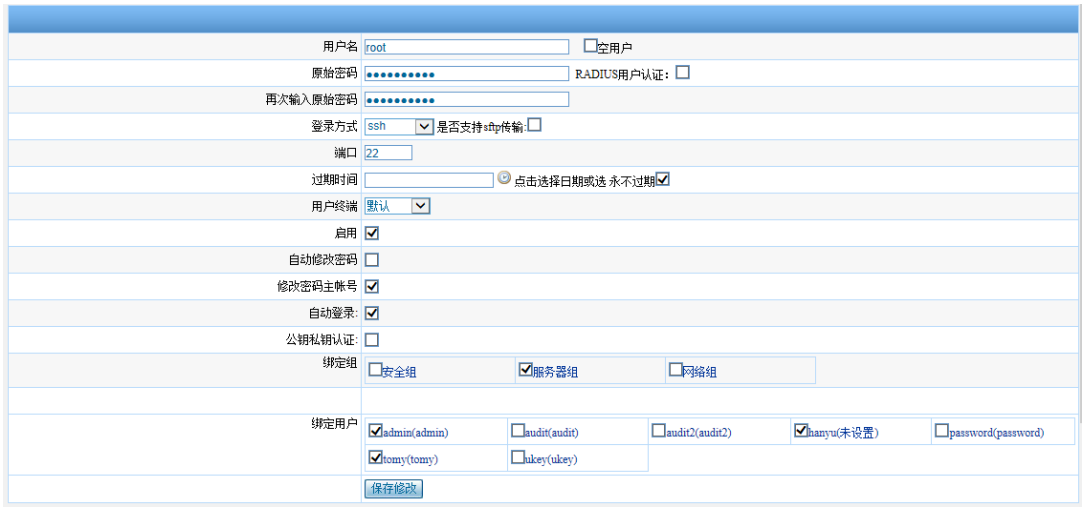
6.1 系统权限查询

在“资源管理-授权查询”菜单页面中，点击“系统权限”选项卡，显示系统权限查询页面，如下图所示。

输入查询条件，比如在输入运维用户名，如下图。

点击“确定”按钮，系统根据输入条件搜索出结果，如下图所示。

如果要修改授权，点击上图列表右侧操作栏中的“编辑”，进入与编辑系统用户相同的界面，可以改变权限绑定关系。

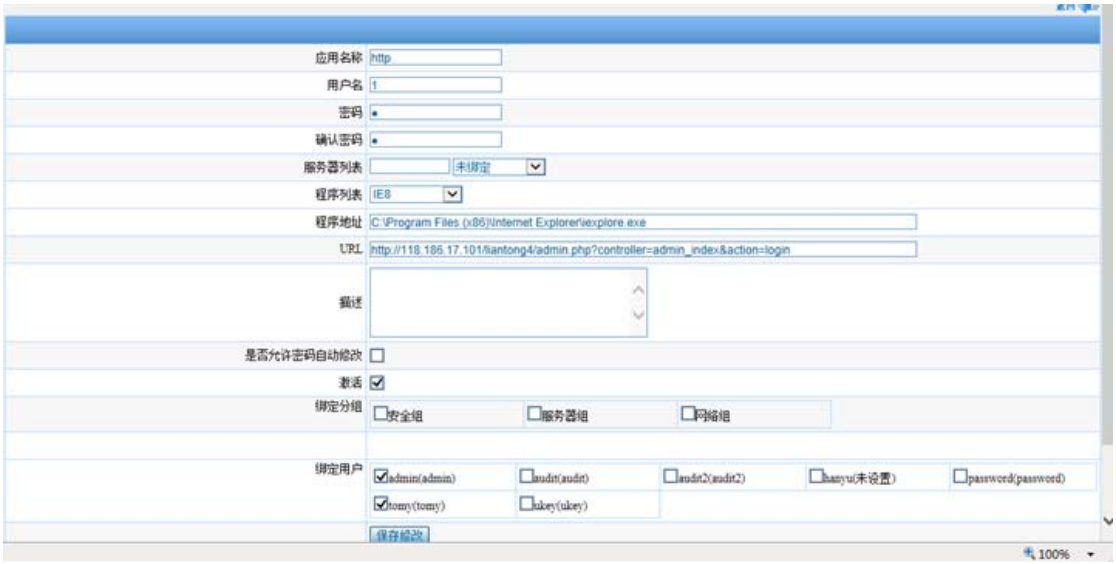


6.2 应用权限查询

在“资源管理-授权查询”菜单页面中，点击“应用权限”选项卡，显示应用权限查询页面，如下图所示。

可以在上图中输入查询条件重新进行筛选。

如果要调整修改应用授权，请在上图中选择目标行，在右侧操作栏点击“编辑”，进入应用发布权限修改界面，如下图所示。



7 策略设置

策略是实现运维控制机制的关键，“策略设置”就是管理员根据实际需要设置各种测试的集中管理模块。

7.1 默认策略

点击“资源管理-策略设置”菜单打开策略设置界面，如下图所示，显示当前默认策略设置。

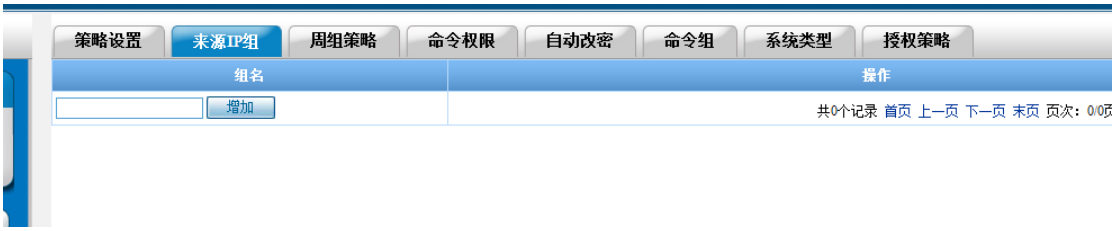
首先看到的是系统默认策略。系统默认策略就是一个模板，在真正绑定策略的时候，可以不加修改地使用它，也可以进行按需的调整后绑定。比如在系统账号绑定运维账号的时候，讲过如何通过点击用户名设置具体的策略。

默认策略中的“周组策略”、“来源 IP 组”、“命令权限”等都需在本页面的其他选项卡中设置好以后才可用。

7.2 来源 IP 组

来源 IP 组的作用是为了对运维终端 IP 进行限制。来源地址限制分为 WebPortal 登录限制和直接使用运维工具限制二部分，WebPortal 登录限制，可以限制用户登录 WEB 界面时的来源地址，运维工具限制可以限制用户使用运维工具直接连接系统时的来源地址，一般情况下，如果对用户来源地址进行限制，建议将 WebPortal 和运维工具限制方式都进行设定。

一个来源 IP 组就是包含多个源 IP 地址的组。下图定义了一个名称为“内网组”的来源 IP 组。



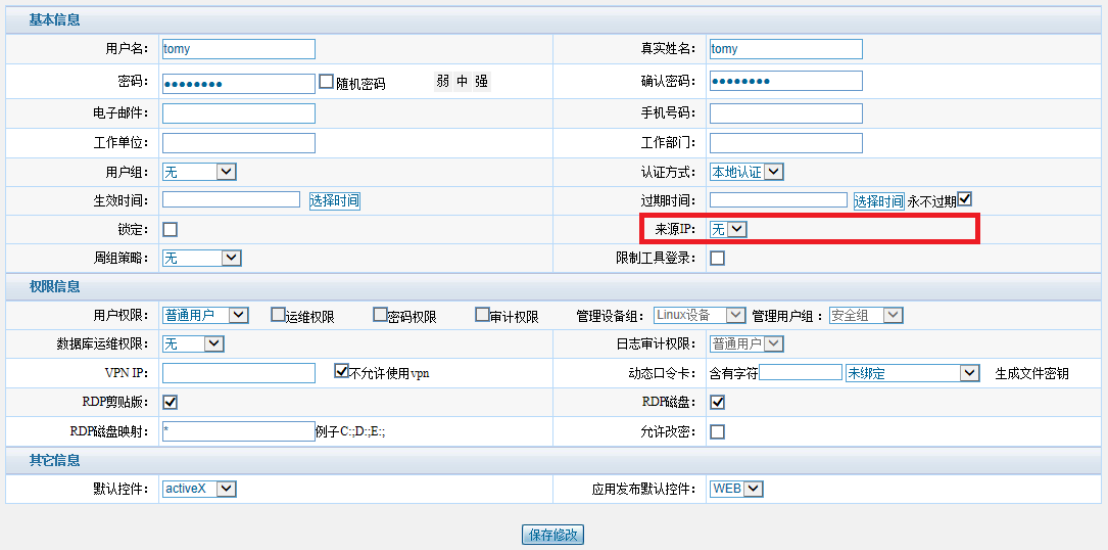
在来源 IP 组管理界面列表操作栏中点击“ip”操作，可以对对应行的来源

IP 组进行编辑，添加或者删除该 IP 组中的 IP 地址，如下图所示。

点击“添加”按钮可以网组中添加一个新的 ip 地址。注意 ip 地址的表示方式，是要带掩码的，如 127.0.0.0/8 或 192.168.1.24/255.255.255.0。

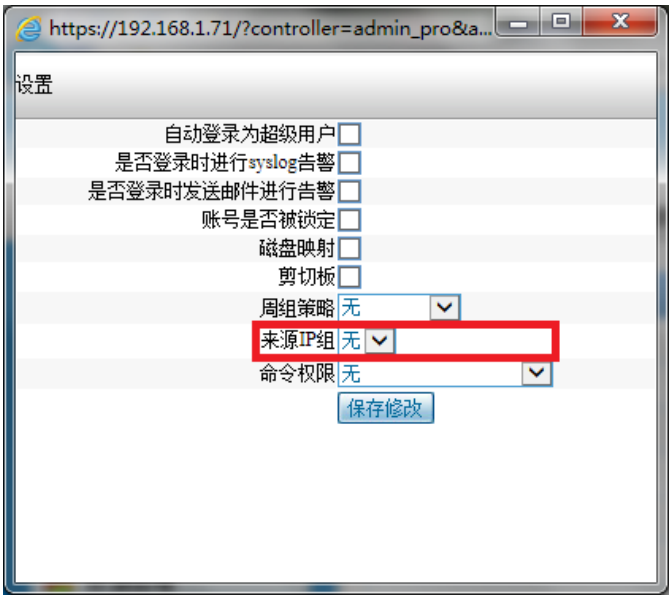
添加 IP 地址需要符合标准掩码模式，比如 192.168.0.0/24 等，如果想添加一个单独的 IP 到地址组，则只需要将掩码设置为 32 位即可。

WebPortal 登录限制在新建和编辑用户时可以设置，如下图所示。



点击保存修改按钮后，以后这个用户只能从绑定的地址组来源里登录，当从其它地址登录时，系统会自动提示并退出。

WebPortal 模式不能禁止运维人员直接使用运维工具登录到目标服务器的方式，如果开启了直接登录方式，则除了 WebPortal 绑定外，还需要对用户登录权限进行绑定限制，可以在系统用户绑定给用户、系统用户组绑定给用户、设备组绑定给用户时的任何一个地方进行来源地址组绑定，如果权限冲突，则系统会遵循以下优先原则，即系统用户组的权限覆盖设备组的，系统用户的覆盖系统用户组的。在做任何一个绑定时，都可以单击用户名或用户组名（**为了避免操作混乱，推荐在系统用户组处绑定**），用户权限绑定对话框如下图所示。



选中来源 IP 组后，点击保存修改按钮，返回到上层权限绑定界面，再次点击保存修改按钮，才可以使设置生效（注意，如果在权限绑定界面没有点击保存修改按钮，则配置不会保存）。

7.3 周组策略

周组策略是一周为周设定访问时间策略的一种方式，可以规定一周中每一天的有效时段，比如定义一个周一至周五每天上午 9 点到下午 18 点的时间策略。下图是已经定义的周组策略列表显示，可以修改或者添加新的。

下图是建立一个新的周组策略的界面，可以很清楚看出周组策略的定义方式。每一天或者给出有效时段，或者选择后面的“全部允许”或“全部禁止”。时段的表示，采用开始时间和结束时间来定义，时间格式是：hh:mm:s s。

7.4 命令组

命令组就是设置的一组命令，可以在“命令权限”策略设置中使用这些命令组，在那里称为命令模板。

点击上图中命令组列表右侧操作栏中的“命令编辑”，可以对现有命令组进行编辑修改，点击“添加”按钮可以建立一个新的命令组。下图是编辑一个命令组的页面。

点击“添加”可以为改组添加命令，一次可以添加多个命令，如下图所示。

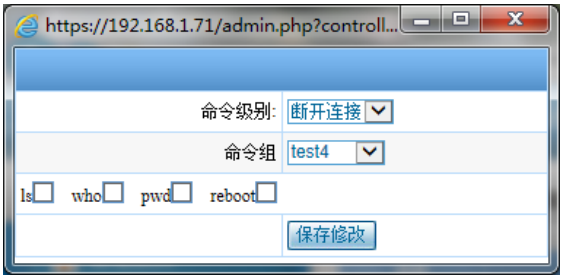
7.5 命令权限

“命令权限”策略设置就是通过设置命令黑白名单，实现命令防火墙的功能，堡垒机根据命令权限策略实时监控操作指令，并根据命令危险级别做出响应。白名单为用户只能执行的命令，即只要做了绑定以后，用户不能执行白名单之外的命令，黑名单为用户不能执行的命令，即做了绑定以后，用户只能运行黑名单之外的命令。对命令的控制，分为断开连接、阻断执行和告警三种方式。下图是“命令权限”配置管理页面。

点击“添加”按钮，可以添加一个新的命令组权限策略，如下图所示，可以选择是白名单还是黑名单。

在命令权限列表页面，点击列表右侧操作栏中的“命令编辑”可以编辑已有命令组权限策略，如下图所示。

点击“从模板添加”就是使用已经定义好的命令组来添加命令，如下图所示。



如果选择直接“添加”命令的方式，操作界面如下图所示，一次可以添加多条命令。

7.6 自动改密

设置自动改密的密码复杂性策略，如下图所示。

7.7 系统类型

系统类型是一个列表，预设运维中使用的设备的操作系统类型，在设备管理的时候可以直接选用，如下图所示。

7.8 授权策略

“授权策略”就是设置控制普通用户访问堡垒机的权限的策略，包括登录时间、会话时长、客户端 IP 等。下图是“登录策略”管理主页面。

点击“修改”或“增加”能够清楚看到一条授权策略的权限控制内容，如下图所示。

8 密码密钥文件

密码密钥文件是系统改密的密码密钥发送邮件记录，如下图所示。

9 系统配置

9.1 参数配置

“参数配置”是配置 iAudit 堡垒机系统满足实际应用环境要求正常运行的系统参数。

9.2 VPN 配置

iAudit 运维堡垒机内置 VPN 服务器设置，采用出厂默认即可，不需要修改。

9.3 系统参数

“系统参数”设置界面如下图所示。

NTP 服务器设置比较重要，用于保持设备与标准时间服务器的同步。

如果在内网没有可用的时间服务器，需要校准系统时间。

FTP 和 SFTP 备份阈值，设置备份文件的大小限制，超过此限制的认为是大文件不备份，小于的进行备份，备份的文件审计员可以查看审计。

SNMP 服务的开启是为给外部管理系统提供管理接口。

9.4 密码策略

“密码策略”配置界面如下图所示。

时间设置：会话空闲时间设置，超过此时间需要重新输入密码。

令牌漂移：动态口令的时候，允许 Key 与后台的时间偏差，图中 30 表示可以前后相差不超过 15 分钟。

9.5 高可用性

在配置 HA 集群的时候，需要在管理控制台进行设置，如下图所示。

浮动 IP ：HA 浮动地址

双机状态：当前双机进程的状态，绿色为启动，红色为停止

从 IP：添从服务器的 IP 地址

Priority:优先级，决定哪台服务器能为主用状态，优先级高的服务器将会优先取得主用状态

9.6 告警配置

“告警配置”设置系统是否启用告警，以及使用的告警方式，系统支持邮件和 syslog 两种告警方式，各项参数配置如下图所示。

9.7 告警参数

告警参数是设置系统各项告警事件的触发门限值，如下图所示。CPU、内存、SWAP、硬盘都是设置百分比，SSH、TELNET、RDP、FTP、DB 告警值都是只会话的并发数。

10 系统管理

10.1 服务状态

查看系统各服务运行状态，并可在界面启动或者停止指定服务，如下图所示。

10.2 系统状态

显示系统当前工作状态、在线用户信息，并以图的方式显示系统资源使用状态，如下图所示。

10.3 配置备份

备份和恢复系统配置，操作界面如下图所示。

点击“生成备份文件”会生成一个 audit_sec.sql.gz 的备份文件。

10.4 数据同步

“数据同步”是实现堡垒就之间的单向同步，一般用在主堡垒机向从堡垒机的同步数据。数据同步的配置项如下图所示。

1. 同步地址：从服务器地址；
2. 同步端口：2288；
3. 数据库同步：一般选择“配置同步”；
4. 审计文件同步：是指是否同步日志文件；
5. 数据库用户和密码：缺省都是 freesvr；
6. 备份目录：一般设为“/”；

7. 手动同步：是执行一次立即同步。

11 VPN 配置

iAudit 运维堡垒机的 VPN 功能主要用于外网运维用户的接入，提供安全的通道，配置比较简洁。

VPN 基本配置，采用默认参数即可，如下图所示为系统出厂默认配置。

“VPN 策略”指的是 VPN 的地址映射策略，这里是一种多对一的映射关系，如下图所示，一个来源地址段到一个目标地址段通过应该映射 IP 来联系。

添加一个映射策略就是设置来源地址段到目标地址段的映射地址，如下图所示：

所有地址表示，均包含掩码。

“VPN 路由”是用于网络跳转，在运维审计环境下一般禁止跳转，不需要配置。

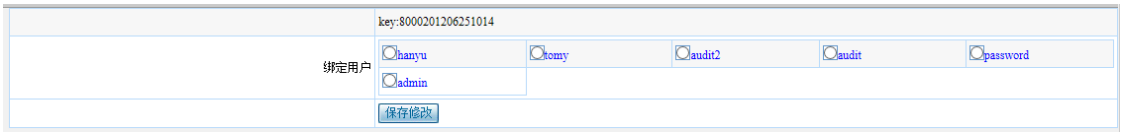
12 动态口令

12.1 USBKEY 导入

使用动态口令进行用户登录认证前，需要把每个 USBKEY 的序列号导入系统，这是通过一个序列文件导入过程完成的，操作界面如下图所示。

12.2 USBKEY 绑定

启用 USBKEY 的第二步，就是把 USBKEY 序列号与用户绑定。具体操作是，在上图的导入序列号列表中，对需要绑定的序列号，点击操作栏的“编辑”操作，选择要绑定的用户，如下图所示。



13 Licnese 管理

iAudit 运维堡垒机的系统功能是受许可限制的，启用堡垒机功能需要导入 License 许可文件。

License 许可文件，与硬件平台一一对应，许可授权堡垒机功能和可管理的

设备数量。

导入 License 之后，不能再修改 MAC、IP、网关，否则 License 失效。

License 许可的申请步骤：

（1） 管理员登录管理控制台生成申请码；

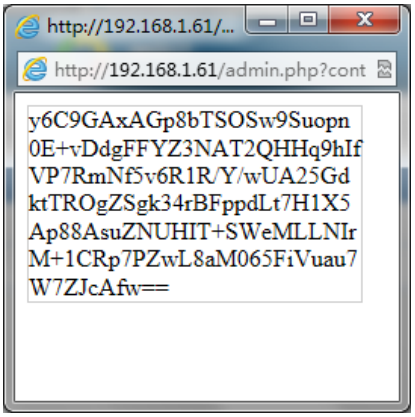
（2） 以电子邮件方式，向销售厂商提出申请，申请邮件中包括申请码和硬件平台序列号；

（3） 收到授权 license 文件；

（4） 将授权 license 文件上传至系统中，导入成功完成授权。

生成申请码和导入许可证文件的界面如下图所示：

申请码是系统生成的一串字符，需要全部拷贝，不能遗漏或增加。



成功导入许可证后，可以看到授权可管理设备数，至此设备可以正式使用了。

14 运维审计

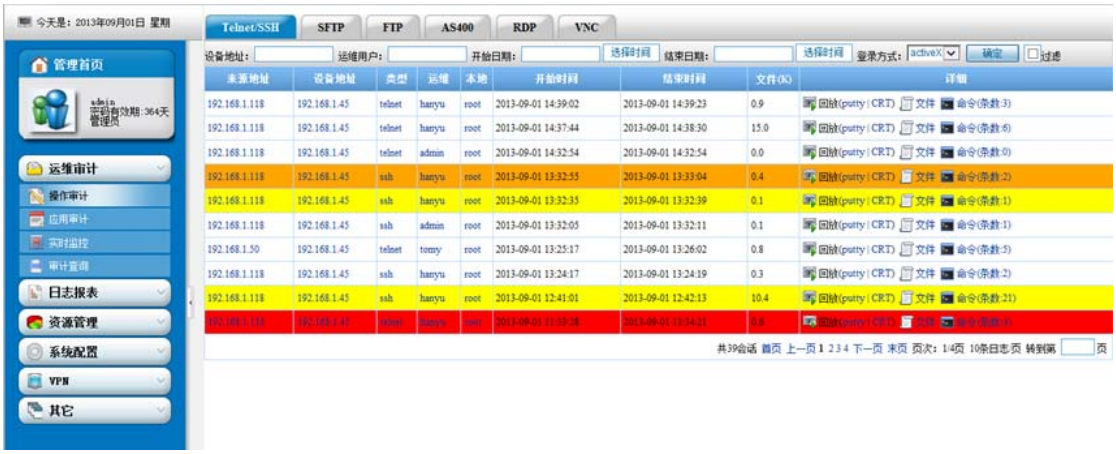
14.1 操作审计

不同的用户拥有不同的操作审计权限，其中管理员和审计员可以审计所以人的操作，普通用户只能审计自己的操作。

14.1.1 字符会话审计（Telnet/SSH）

Telnet 和 SSH 会话属于字符会话，这类协议的特点是以字符命令操作为主，命令防火墙对这类协议效果最好。

如下图所示，会话列表以颜色表示不同会话的状态。



白色会话行：正常会话；

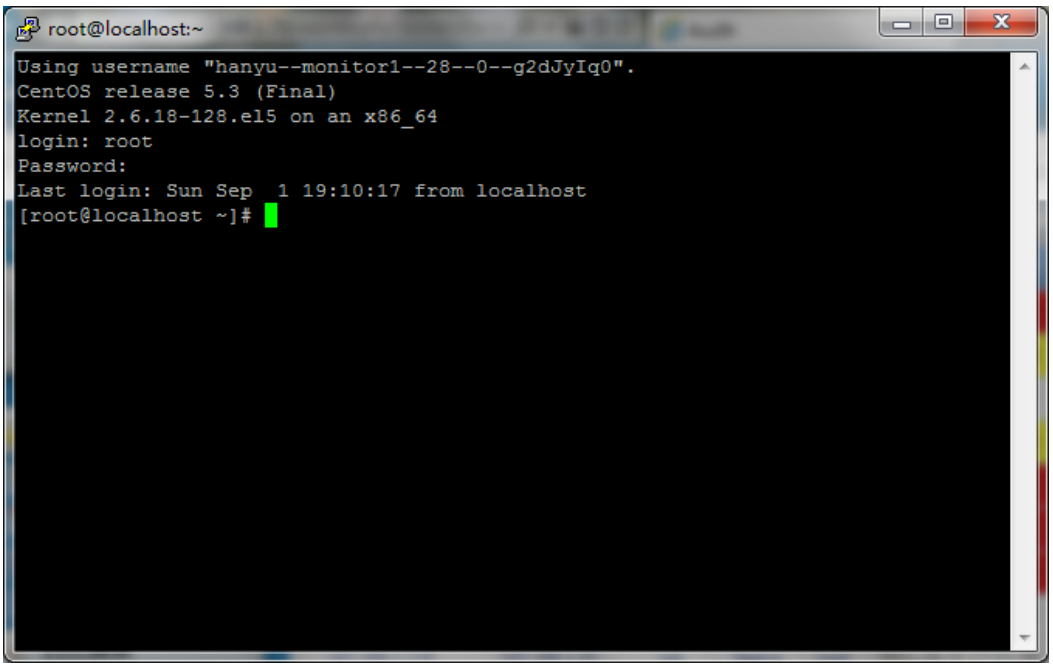
黄色会话行：会话中有告警级别的命令操作；

橙色会话行：会话中有被阻断执行的命令；

红色会话行：会话有违规操作被断开；

■ 回放审计

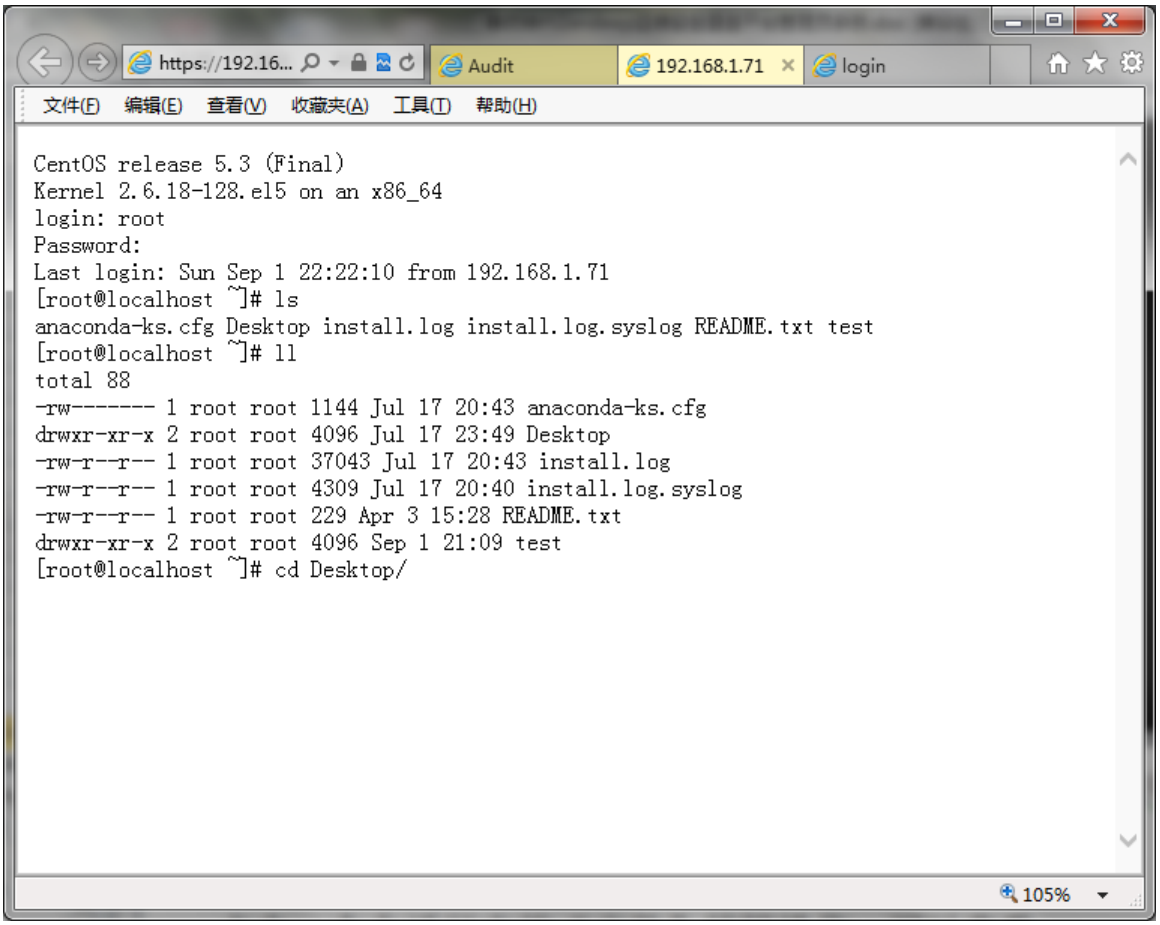
点击会话列表中一行中的“回放（putty|CRT）”可以进行回放审计，下图就是回放画面。



其中按下**空格键**可按每键盘输入回放、按下**回车**可按每命令输入回放。

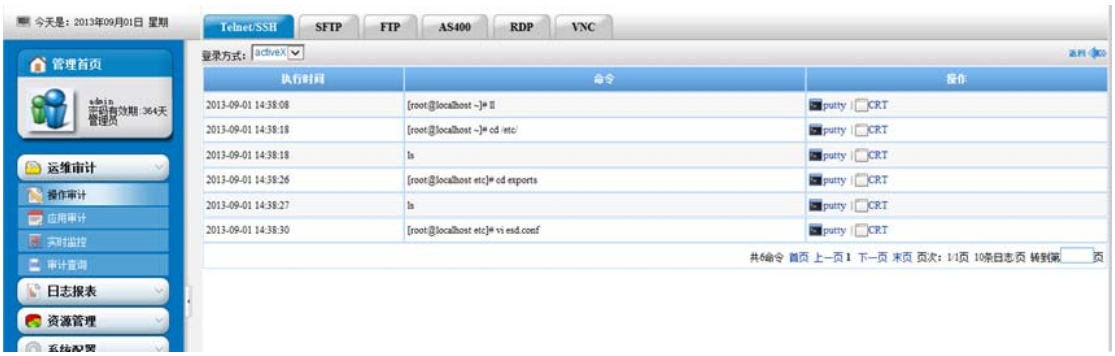
■ 命令记录查看

点击一个会话行中的“文件”按钮操作，可以查看会话过程中输入的全部命令和执行结果，如下图所示。



■ 命令列表式查看

点击任何会话行中的“命令”操作按钮，将以列表的方式显示该会话执行的全部命令，如下图所示。



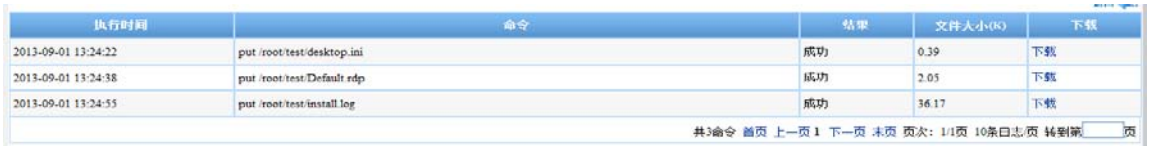
命令列表每行一条命令，点击命令行右端操作栏中的“Putty”或者“CRT”可以开始从命令处进行回放。

14.1.2 SFTP 和 FTP 会话审计

FTP 和 SFTP 会话都是文件传输操作会话，对这两类会话除了可以审计会话用户、时间、来源、目标、操作命令，iAudit 堡垒机还可以审计上传和下载的文件。

SFTP/FTP 会话列表包含信息如下图所示。

点击“查看”能够查看一个文件传输会话过程中所有的操作命令列表，如下图所示。



最右边一列“下载”栏中有下载链接的，表明该行命令有文件传输操作，并且文件已经被备份了，可以下载下来进行审计。

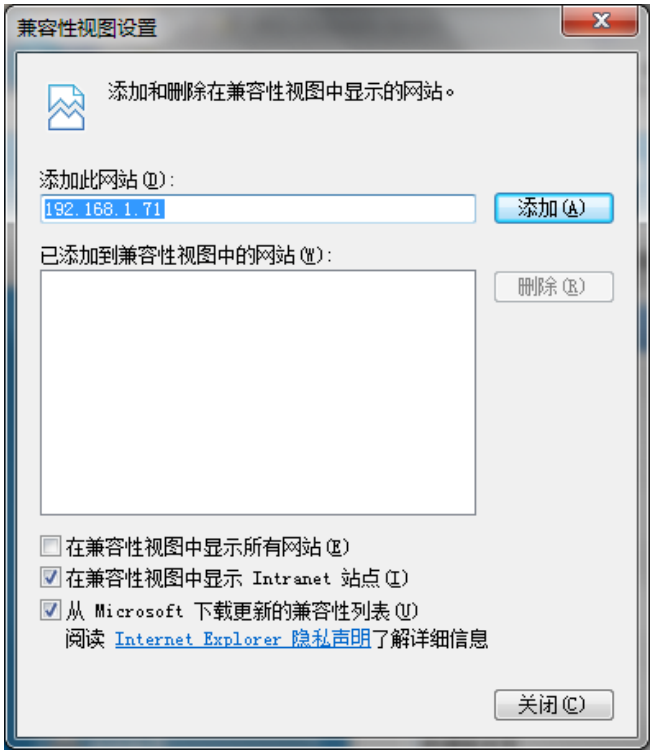
14.1.3 图形会话审计

RDP 和 VNC 会话都属于图形会话，操作基本以鼠标点击为主，也有键盘输入信息。

RDP 和 VNC 会话回放审计需要 JRE 支持。回放支持两种方式，一种是独立窗口回放，一种是 ActiveX 控件在 IE 浏览器窗口回放。

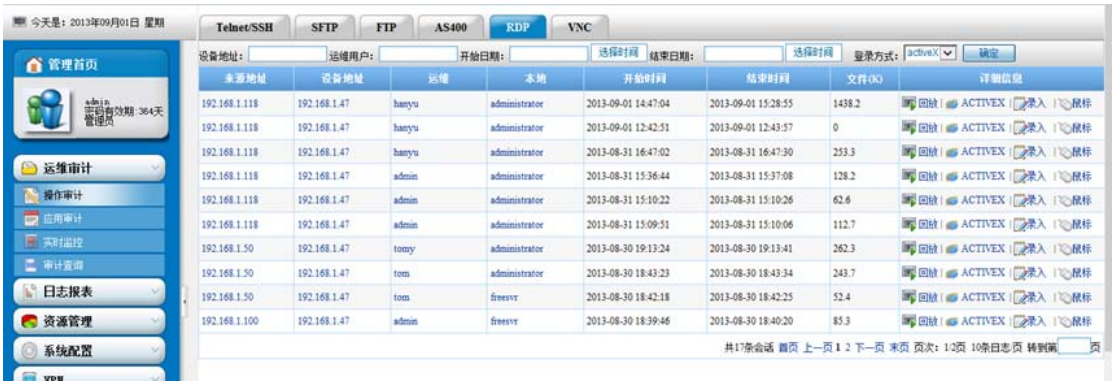
使用 ActiveX 在 IE 窗口回放时，如果感觉不顺畅，可以启用浏览器的“兼容视图”，如图所示点击地址栏图标。

兼容性视图也可以在 IE 菜单—工具—兼容性视图设置中配置，如下图。



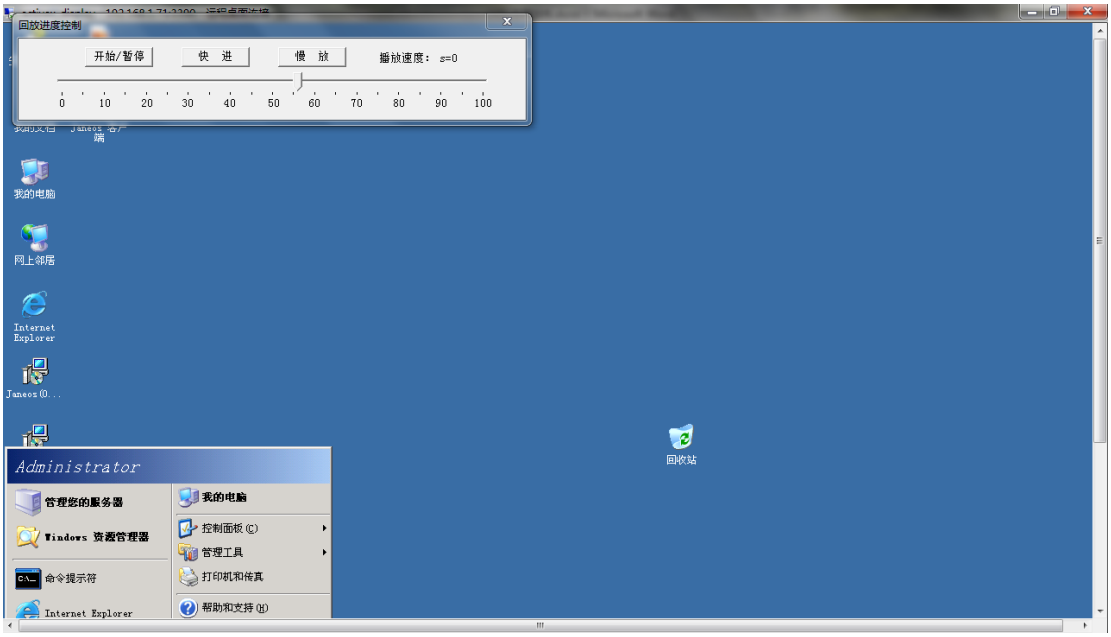
14.1.3.1 RDP 会话审计

RDP 会话列表如下图所示。

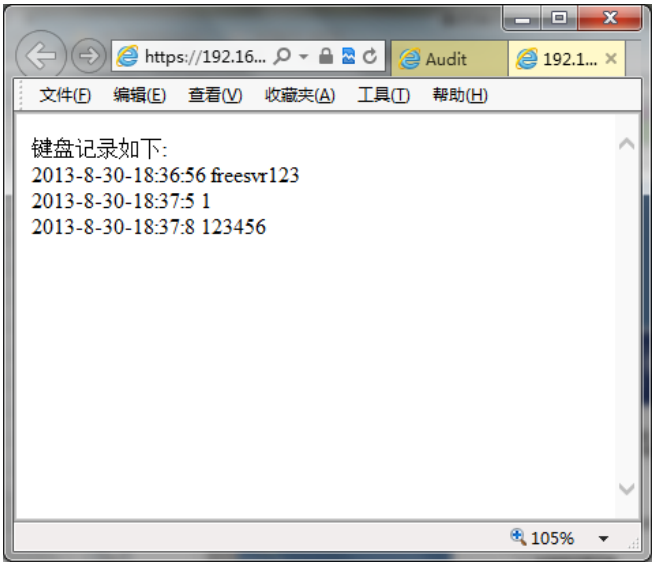


从每个会话可以审计来源 IP、设备 IP、运维用户、系统账号、开始时间、结束时间等。

点击“回放”按钮和 ActiveX 按钮都可以全过程回放会话过程，区别是，直接“回放”是在独立的本地窗口进行回放，而 ActiveX 方式是在浏览器窗口中进行回放，下面两个图可以看出两者的差别，回放效果相同，从方便性上，可能直接回放更方面，不需要对浏览开放更多的控件许可。



RDP 会话列表中的“录入”可以查看键盘操作信息，如下图所示。



RDP 会话列表中的“鼠标”可以查看鼠标点击操作信息，如下图所示。

Telnet/SSH | SFTP | FTP | AS400 | RDP | VNC

返回

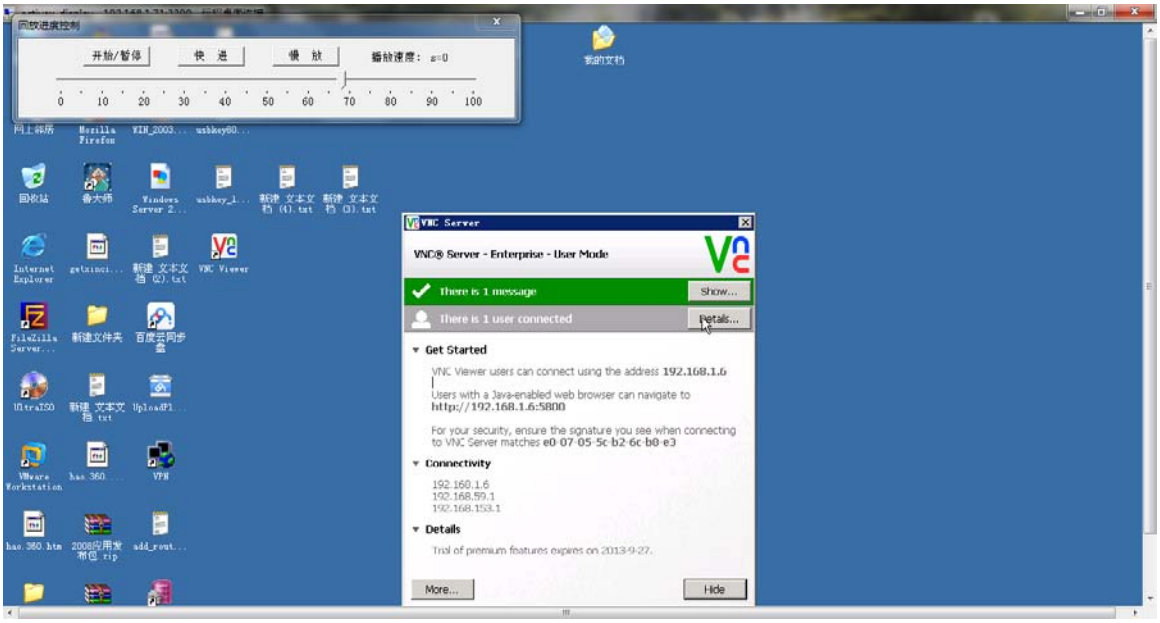
点击时间	坐标位置	鼠标键	动作
2013-08-30 19:13:31	796*551	左键	按下
2013-08-30 19:13:31	796*551	左键	放开
2013-08-30 19:13:32	406*738	左键	按下
2013-08-30 19:13:32	406*738	左键	放开
2013-08-30 19:13:32	409*746	左键	按下
2013-08-30 19:13:32	409*746	左键	放开
2013-08-30 19:13:34	1026*180	左键	按下
2013-08-30 19:13:34	1026*180	左键	放开
2013-08-30 19:13:35	19*937	左键	按下
2013-08-30 19:13:35	19*937	左键	放开

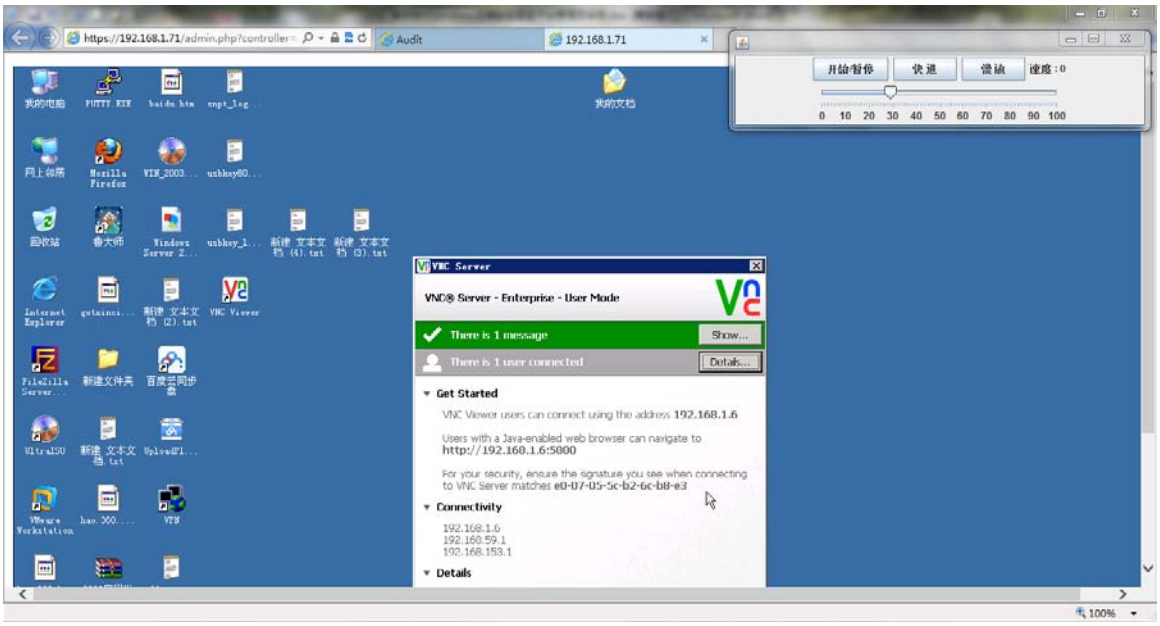
共14命令 首页 上一页 1 2 下一页 末页 页次：1/2页 10条日志 页 转到第 页

14.1.3.2 VNC 会话审计

VNC 会话列表如下图所示，与 RDP 不同的是有一列流量统计。

与 RDP 会话类似，点击“输入”可以查看键盘操作信息，点击“回放”和 ActiveX 都可以实现会话过程的回放，ActiveX 方式是在网页中回放，两种方式的回放如下面两个图所示。



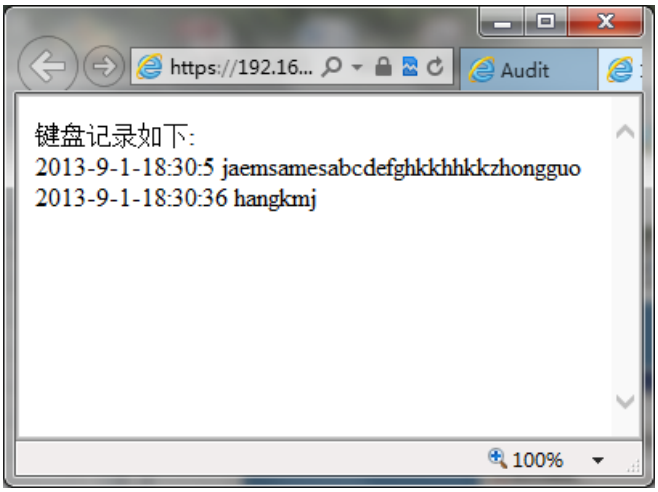

VNC Server
VNC® Server - Enterprise - User Mode
There is 1 message
Show...
There is 1 user connected
Details...
Get Started
VNC Viewer users can connect using the address 192.168.1.6
Users with a Java-enabled web browser can navigate to
http://192.168.1.6:5800
For your security, ensure the signature you see when connecting to VNC Server matches e0-07-05-5c-b2-6c-b8-e3
Connectivity
192.168.1.6
192.160.59.1
192.168.153.1
Details

14.1.4 应用审计


应用发布
管理首页
运维审计
操作审计
应用审计
实时监控
审计查询
日志报表
资源管理
系统配置
VPN
其它


回放进度控制
开始/暂停
快 退
慢 放
播放速度：s=0
0 10 20 30 40 50 60 70 80 90 100
登录QQ邮箱
QQ邮箱
mail.qq.com
English | 反馈建议 | 帮助中心 | 企业邮箱
QQ邮箱，常联系！
从明天起，和每个亲人通信
告诉他们我的幸福
那幸福的闪电告诉我的
我将告诉每个人
摘自 海子《面朝大海 春暖花开》
登录QQ邮箱
@qq.com
QQ密码
记住登录状态
忘记密码？
登录
还没有QQ邮箱？立即注册
网络太慢？使用基本版
关于腾讯 | 服务条款 | 客服中心 | 联系我们
完成
Internet | 保护模式: 禁用
100%


https://192.168.1.71/admin.php?controller=
Audit
192.168.1.71
开始/暂停
快 进
慢 放
速度：0
0 10 20 30 40 50 60 70 80 90 100
登录QQ邮箱 - Windows Internet Explorer
https://mail.qq.com/
登录QQ邮箱
QQ邮箱
mail.qq.com
English | 反馈建议 | 帮助中心 | 企业邮箱
QQ邮箱，常联系！
从明天起，和每个亲人通信
告诉他们我的幸福
那幸福的闪电告诉我的
我将告诉每个人
摘自 海子《面朝大海 春暖花开》
登录QQ邮箱
@qq.com
QQ密码
记住登录状态
忘记密码？
登录
还没有QQ邮箱？立即注册
网络太慢？使用基本版
100%



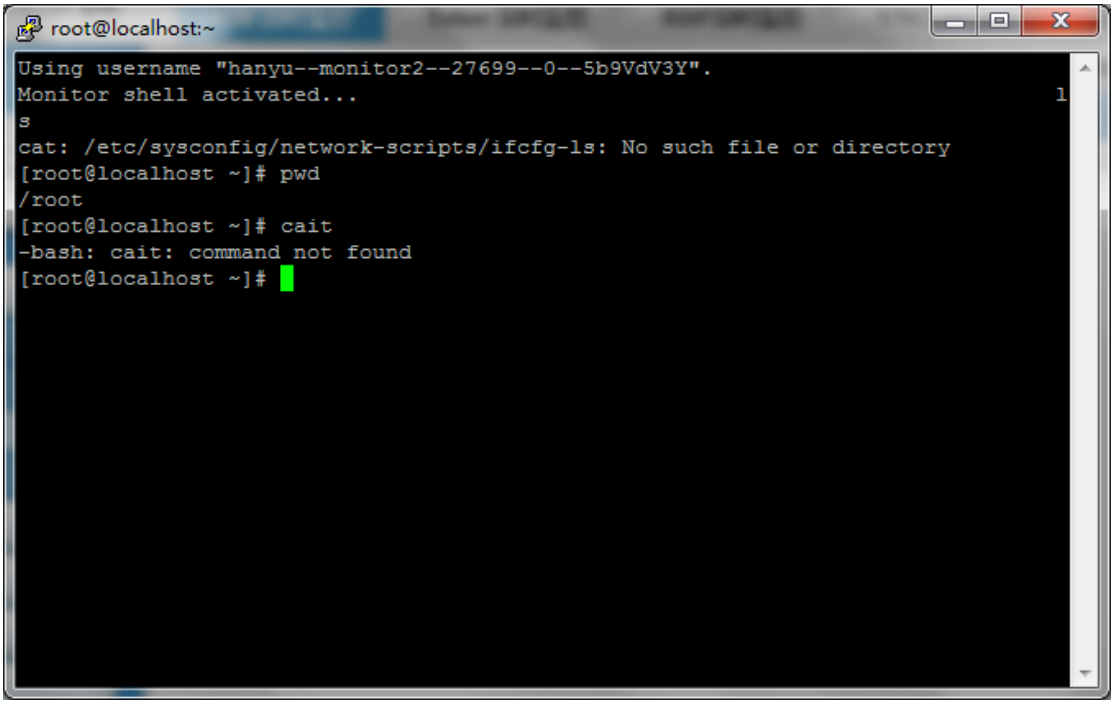
14.2 实时监控

Zeendeep 运维堡垒机支持运维用户操作的实时监控审计。监控审计的操作内容就是两个：实时监控、断开会话。断开会话只有当认为当前被监控处于危险操作中，不适用于继续下去的时候才会断开它，认为正常的会话可以放弃继续监控。

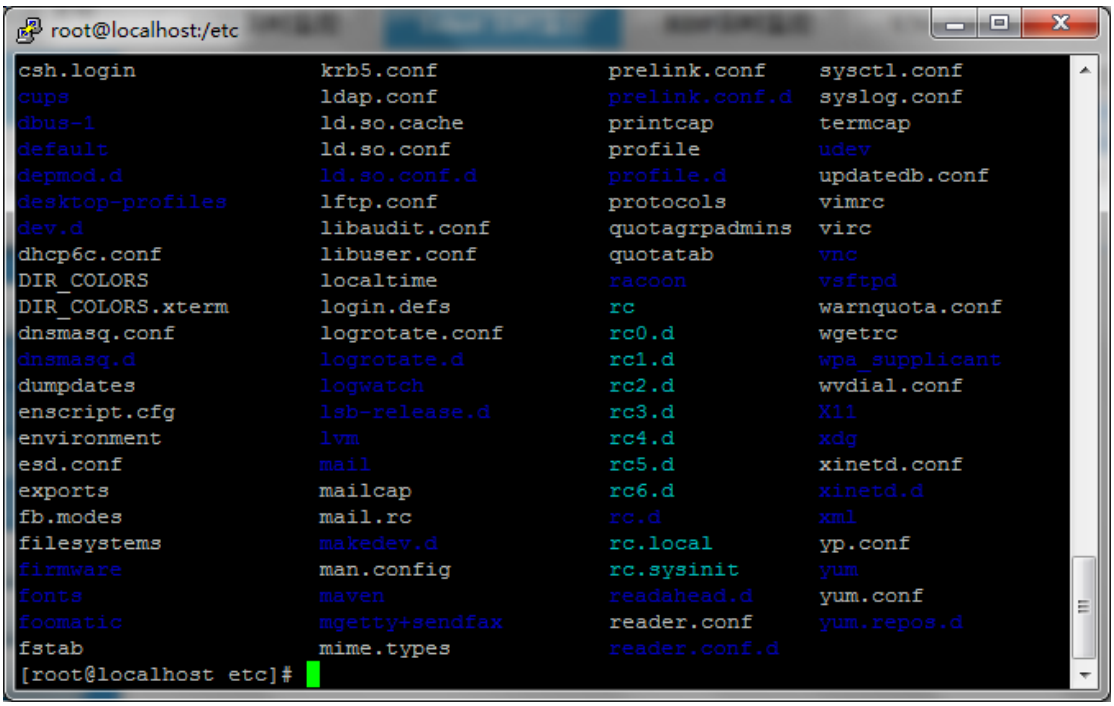
监控的操作跟审计回放有点类似，有的会话也支持 Web 方式监控。

下面把几种不同协议类型会话的监控画面展示一下。

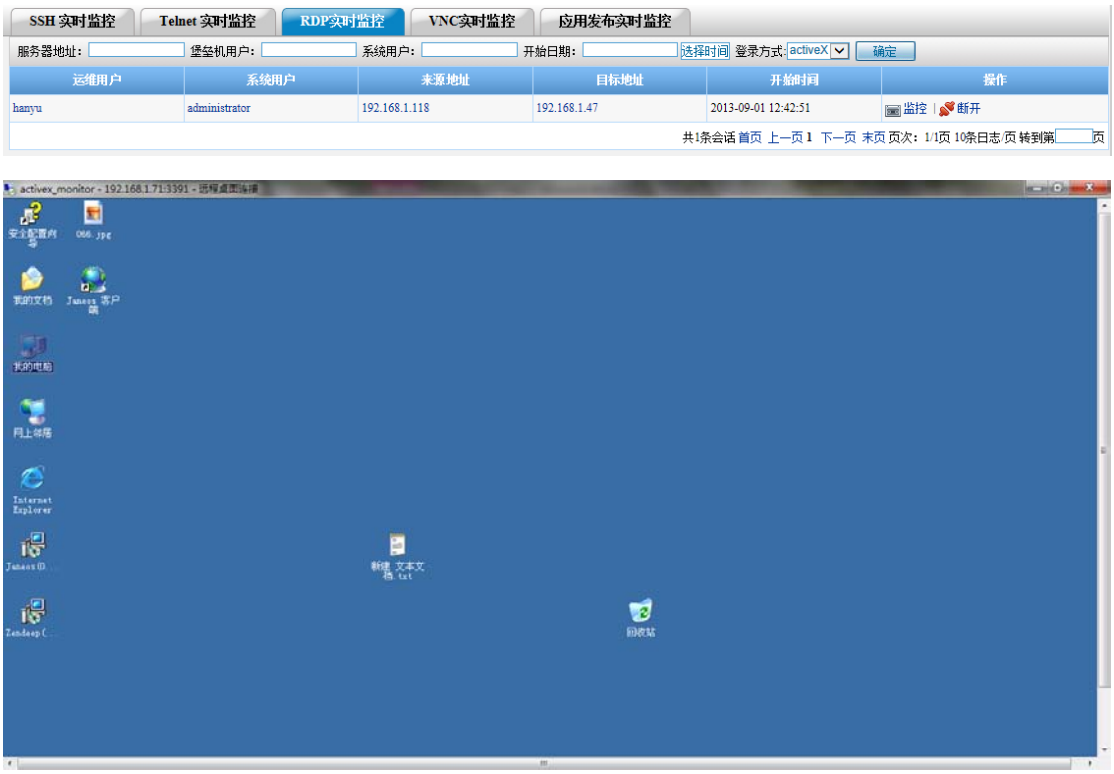
■ SSH 监控



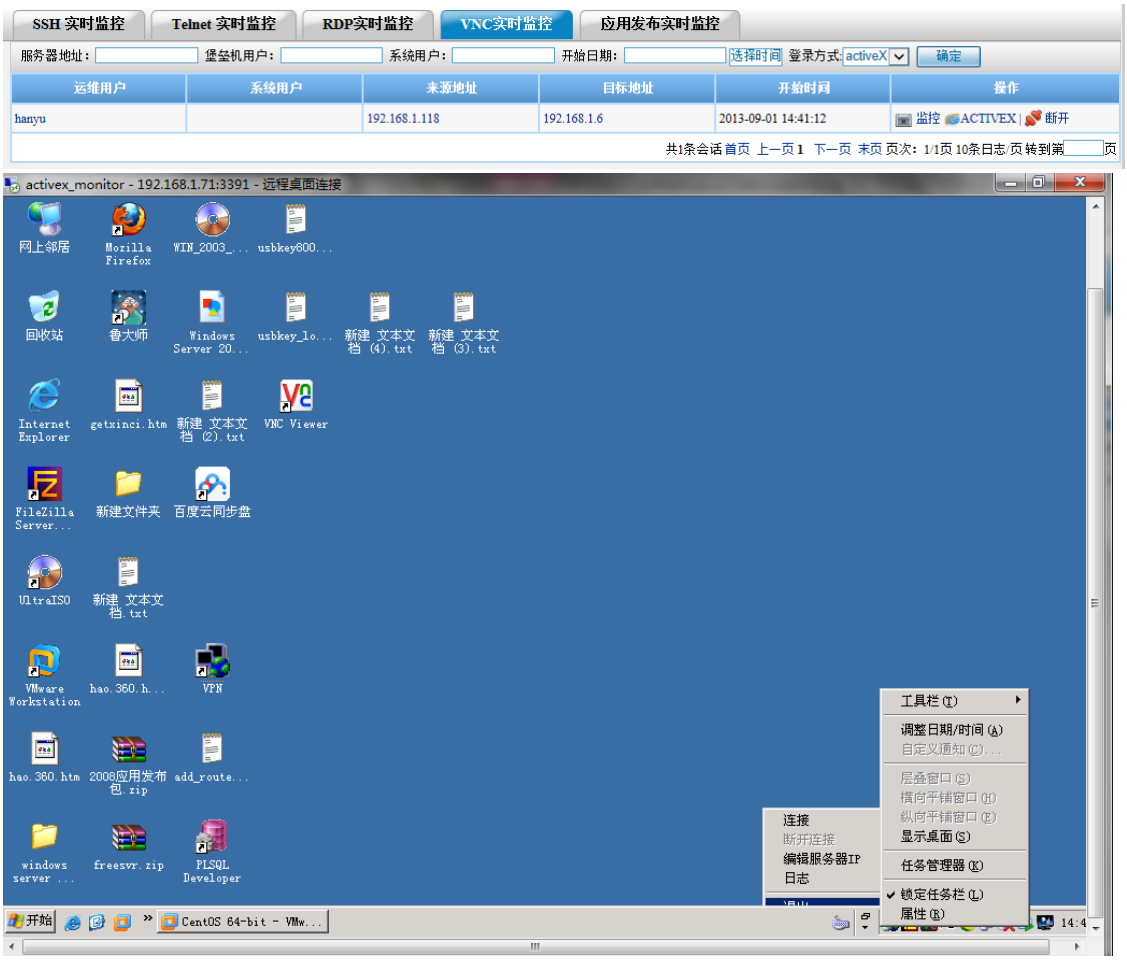
■ Telnet 监控



■ RDP 监控


SSH 实时监控
Telnet 实时监控
RDP实时监控
VNC实时监控
应用发布实时监控
服务器地址：
堡垒机用户：
系统用户：
开始日期：
选择时间
登录方式:
activeX
确定
运维用户
系统用户
来源地址
目标地址
开始时间
操作
hanyu
administrator
192.168.1.118
192.168.1.47
2013-09-01 12:42:51
监控 | 断开
共1条会话 首页 上一页 1 下一页 末页 页次：1/1页 10条日志/页 转到第 页

■ VNC 监控


SSH 实时监控
Telnet 实时监控
RDP实时监控
VNC实时监控
应用发布实时监控
服务器地址：
堡垒机用户：
系统用户：
开始日期：
选择时间
登录方式:
activeX
确定
运维用户
系统用户
来源地址
目标地址
开始时间
操作
hanyu
192.168.1.118
192.168.1.6
2013-09-01 14:41:12
监控 ACTIVEX | 断开
共1条会话 首页 上一页 1 下一页 末页 页次：1/1页 10条日志/页 转到第 页
activex_monitor - 192.168.1.71:3391 - 远程桌面连接
网上邻居
Mozilla Firefox
回收站
鲁大师
Internet Explorer
getxinci.htm
新建 文本文档 (2).txt
VNC Viewer
FileZilla Server...
新建文件夹
百度云同步盘
UltraISO
新建 文本文档.txt
VMware Workstation
hao.360.h...
VPN
hao.360.htm
2008应用发布包.zip
add_route...
windows server ...
freesvr.zip
PLSQL Developer
工具栏(T)
调整日期/时间(A)
自定义通知(C)...
层叠窗口(S)
横向平铺窗口(H)
纵向平铺窗口(E)
显示桌面(S)
任务管理器(K)
锁定任务栏(L)
属性(R)
连接
断开连接
编辑服务器IP
日志
开始
CentOS 64-bit - VMw...

■ 应用发布监控

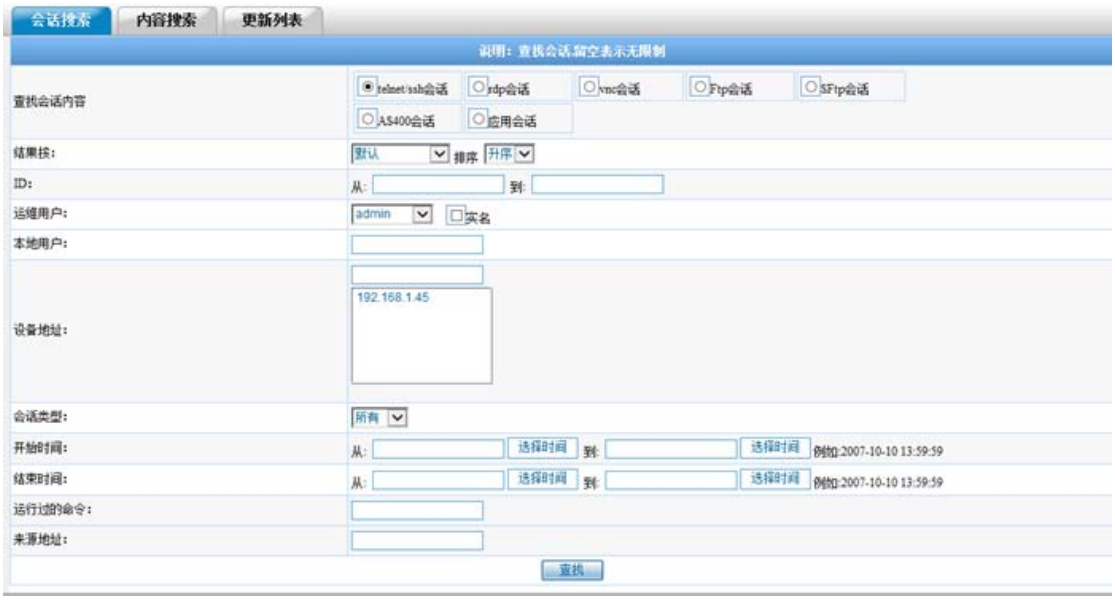
14.3 审计查询

审计查询页面有三个选项卡：“会话搜索”、“内容搜索”、“更新列表”。其实真正用于审计查询的是前两个，“更新列表”其实起一个按钮的作用，对“命令搜索”、“内容搜索”有效。当“命令搜索”或“内容搜索”页面上有一些下拉列表、列表框的时候，如果这些列表中的数据可能在系统的其他地方发生改变，比如设备列表可能被其他管理员修改，这时候点击“更新列表”能够把页面上的列表数据进行更新同步。

14.3.1 会话搜索

“会话搜索”能够通过多种条件组合，缩小范围快速搜索到关心的会话列表。

打开“会话搜索”选项卡页面，如下图，可以看到众多的搜索条件。



下图是搜索运行过 SU 命令的所有 Telnet/SSH 会话的搜索结果。对这个搜索结果会话列表，会明显提高审计的效率。

14.3.2 内容搜索

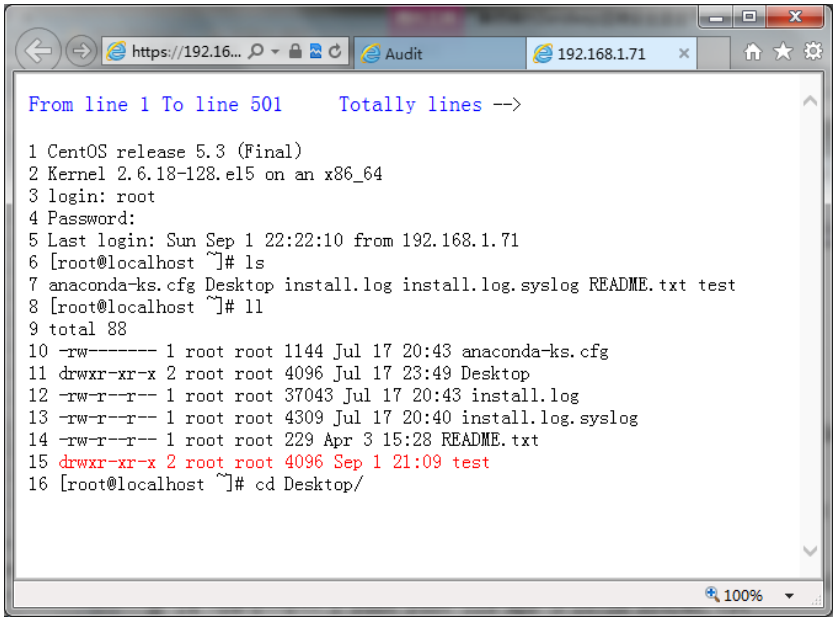
系统还支持内容搜索，即通过输出内容或操作内容进行比对，方便快捷的完

成对敏感操作的审计。此功能对字符会话意义特别大，能够实现全屏内容搜索。

例如，下图是搜索含内容“test”的字符会话信息。

搜索结果如下：

结果会话列表中的日志文件就是会话的输入输出操作记录，点击第一行的日志文件，显示如下图，第 7 行末尾就是搜索的内容“test”。



15 日志报表

“日志报表”是将运维操作的从运维账号、系统账号、登录时间等一系列数据的记录统计，并根据需求生成相应的报表的功能。系统支持多种报表类型：

1. 权限报表
2. 登录报表
3. 操作报表
4. 违规报表
5. 统计图表

其中每一类还有分子类，形成一个报表体系。

对报表的操作主要是两个：

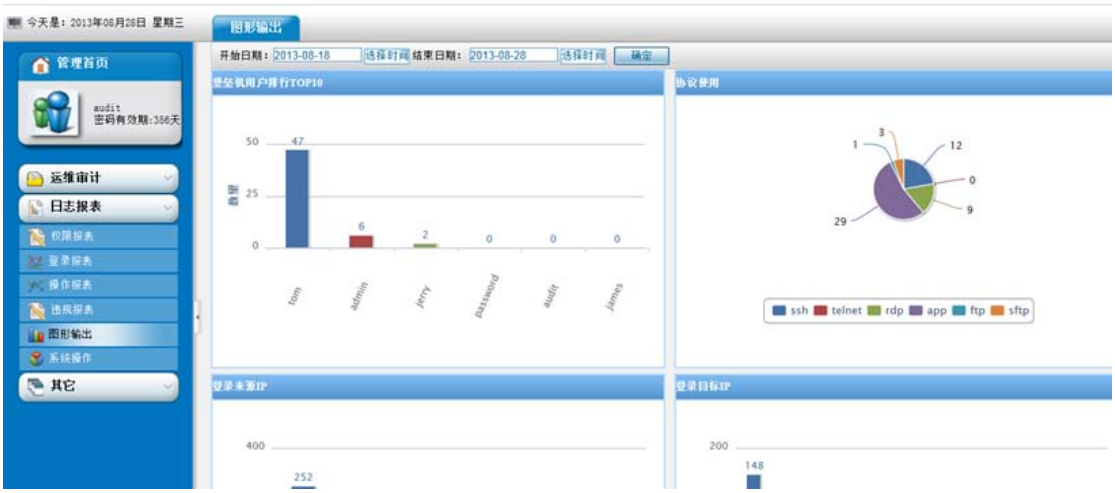
1、 报表数据内容的筛选和数据时间范围的选择

2、 报表导出，系统支持 Excel 和 HTML 两种导出格式

比如权限报表就是通过选择数据内容生成报表：

登录报表就是通过选择时间范围来生成报表：

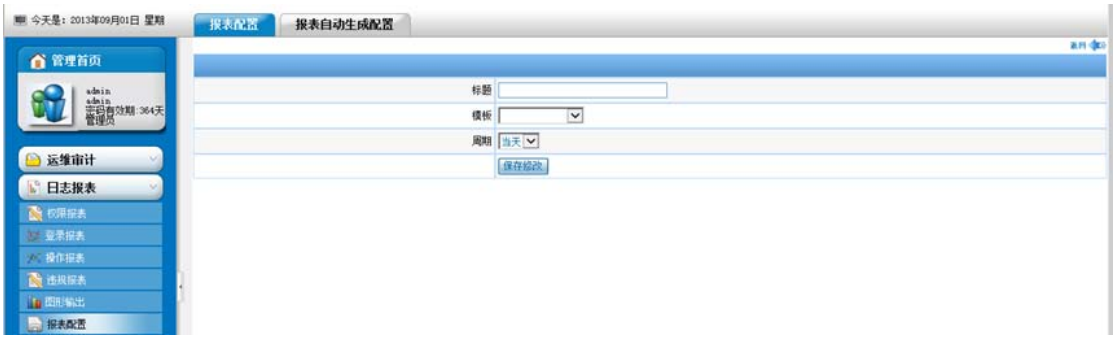
图像报表，是通过直观的柱状图和饼图展示统计数据：



报表配置

报表配置让用户根据自己的需要配置报表，形成一个报表体系，并且可以定期自动生成这些报表。

首先是自定义报表格式，界面如下图。



输入合适的标题，在模板处选择报表模板（包括：统计报表，登录报表，运行命令报表，ftp/sftp 命令报表，应用报表，登录统计、明细、尝试报表）周期是以日、周、月为周期来选择报表的输出。

第二步是定义报表的生成模式，如下图所示。

16 个人信息修改

在“其他”这个菜单里面有个人信息管理，界面如下。

在这里可以修改自己的个人信息，包括自己密码的修改，基本信息的配置修改，其中 RDP 分辨率是指进行 RDP 操作时的默认屏幕分辨率，RDP 映射是对连接 RDP 时的一个映射盘的选择。默认控件是使用 web 登陆系统时的控件选择。