1 概述

中远麒麟 SSL VPN 系统（以下简称 VPN 系统）是用于远程接入的 SSL VPN 产品，产品是开源软件 OPENVPN 的封闭产品，麒麟 VPN 中除了动态口令外其它功能均为免费开源，如果不需要使用动态口令，可以免费使用该产品，并且可以得到产品代码进行定制修改。

1.1 功能介绍

SSL VPN 为封闭开源软件 OPENVPN 的产品，主要修改如下：

1. 界面完全 Web 化，包括加用户、删除用户、配置路由及 VPN 参数
2. 内置开发了麒麟动态口令，用户可以使用 APP 输入动态口令连接，支持 IOS 和安卓二个版本
3. 增加 VPN 管理功能，可以在线查看 VPN 用户，并且可以将不正常的用户踢下线
4. 修改 OPENVPNGUI,让 GUI 完全图形化，不需要手工修改配置文件

2 系统初始设置

2.1 环境要求

麒麟堡垒机要求 ECS 主机内存至少 2G（含 2G），硬盘 20G 以内（含 20G），网卡带宽以并发进行计算，一般应用一个并发为 100K 带宽。

麒麟堡垒机 SSL VPN 使用 TCP 8443、443 二个端口，其中 TCP 8443 为 SSL 需 VPN 端口，供 VPN 连接使用，TCP 443 为 HTTPS 端口，管理员设置用户，普通用户修改密码使用，要将公网访问的 TCP 8443 端口打开。

1、 安装后登录

SSL VPN 系统管理采用 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://SSLVPN 系统 ip

管理员的账号和密码是“admin/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。

麒麟 VPN 系统管理设置主要有二步，一步是添加 VPN 用户，一步是设置 VPN 路由，添加 VPN 用户用于设置哪些用户可以使用 VPN 服务，添加 VPN 路由为可以访问哪些内网资源，如果不添加 VPN 路由，则用户连接 VPN 后，不能访问任何内网资源。

3 目录管理

3.1 目录说明

目录可以认为是用户组，用户组可以是单层结构，也可以是多层结构（目录中包含目录），目录除了管理时检索使用并没有其它的做用，所有的目录中的用户都是一样的。

系统上线前最好划分好目录结构，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，建议使用多层目录。

3.2 目录创建

目录创建时，直接在目录管理菜单，点击添加新节点，输入名称点确定按钮即可。

4 账号管理

4.1 用户角色

麒麟 SSL VPN 设置了二种角色：超级管理员和普通用户，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 目录管理 系统级配置管理
普通用户	SSL VPN 登录、网页修改密码

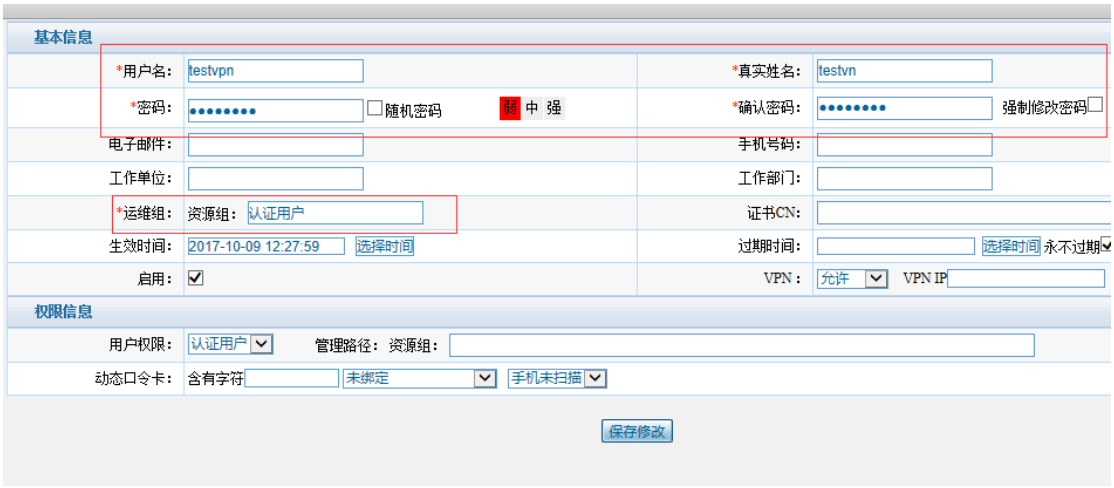
4.2 普通账号管理

4.2.1 添加用户

点击左侧菜单“资源管理—用户管理”，打开用户管理管理界面。初始界面可以看到管理员账号，点击添加按钮可增加一个用户,其中红框勾选的五项为必填项，运维组就是目录管理中的创建的目录。右下角有 VPN 选项，可以选择是否允许 VPN 及用户 VPN 后固定的 IP，如果没有设置 VPN IP，则用户 VPN 后获取的 VPN 地址为 DHCP 随机分配。

注意：建议不对用户进行固定 IP 分配，如果必须分配固定 IP，则 IP 地址必须为 VPN 池中的 IP，并且给每个用户分配了 IP 后，需要到系统管理中重启 VPN 服务才能生效。

用户建议后，即可以用这个用户登录 VPN 系统访问内网资源。



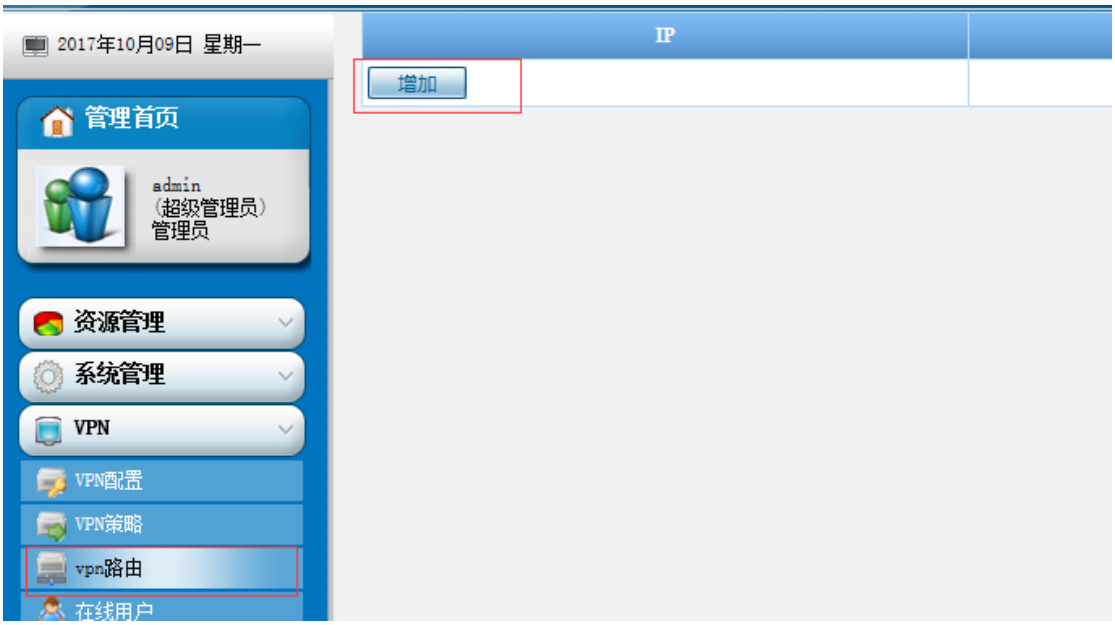
4.2.2 批量添加用户

如果用户非常多的时候，可以用导入方式一次创建大批用户，在导入前，首先要创建一个 VPN 用户做为模版（否则导出为空表头，没有添加示例），然后点击导出按钮导出一个 EXCEL 的 CSV 格式表，然后编辑表，将用户、密码按头一列进行编辑，加入用户后，把头一列删除 ，然后点击导入，将 CSV 表格导入，即可以一次建立大批量的用户。

5 VPN 路由配置

VPN 基本配置中，如果不熟悉参数建议全部使用默认，如果更改可能造成系统无法使用，默认情况只需要增加 VPN 路由即可，VPN 路由就是用户 VPN 后可以访问到的设备和网段。

在菜单 VPN-VPN 路由中点击添加按钮：



输入网段、掩码后，点击保存修改按钮（注意，如果是单个 IP，IP 里添整个 IP，掩码为 255.255.255.255）

用户新连接 VPN 时就会可以访问到添加的网段。

6 其它配置

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 VPN 设备时间的准确性。

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。

7 系统管理

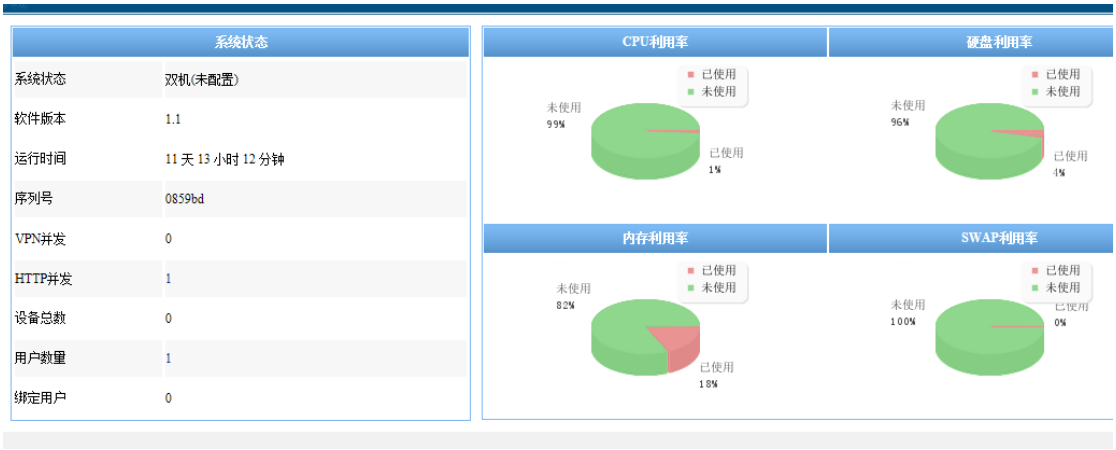
7.1 服务状态

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，位于系统管

理-服务状态菜单如下图所示。

7.2 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。



7.3 配置备份

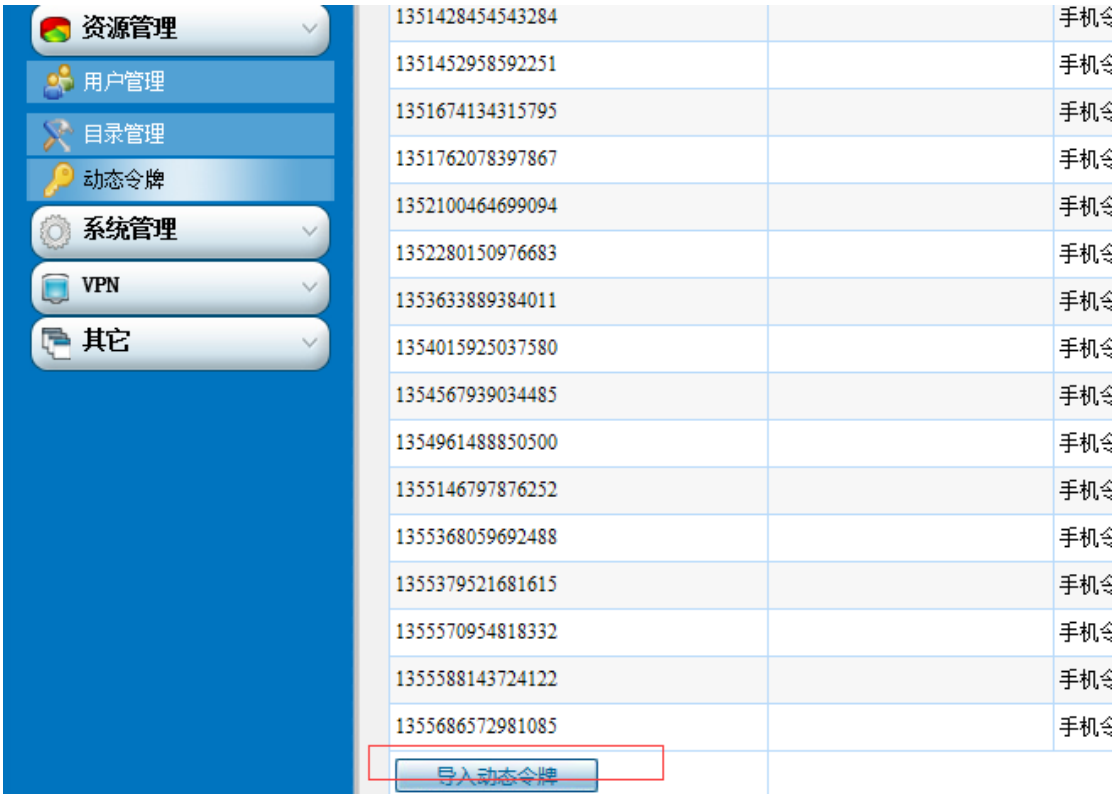
VPN 的配置主要是帐号和密码，如果要进行配置备份，只要在资源管理-用户管理中，点击导出，将用户帐号导出即可，当安装新的堡垒机时，把文件导入。

8 动态令牌

8.1 令牌导入

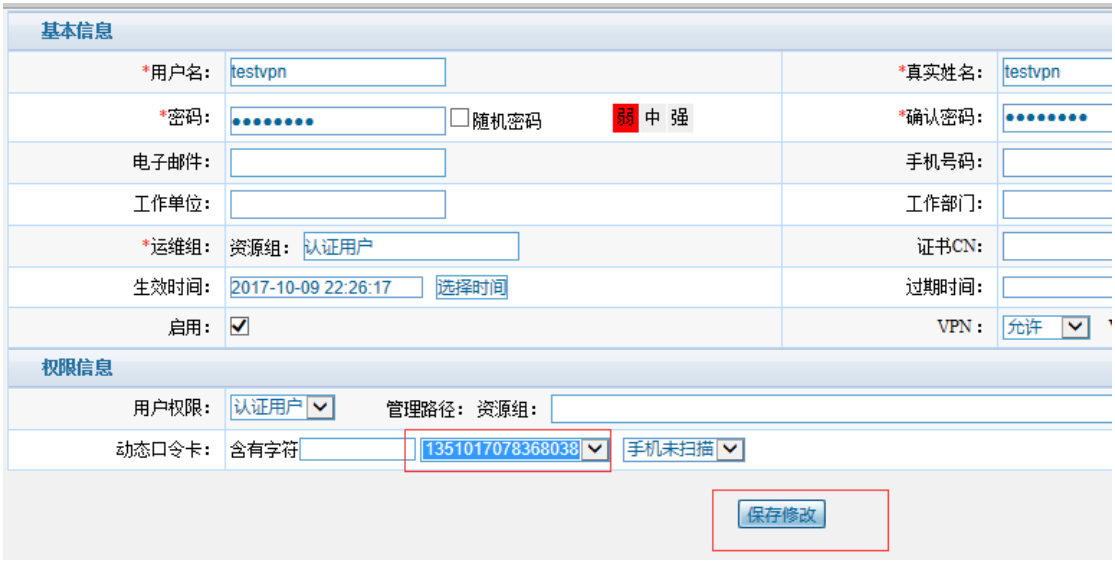
使用动态口令进行用户登录认证前，需要把每个令牌的序列号导入系统，这是通过一个序列文件导入过程完成的，操作界面如下图所示。

资源管理-动态令牌菜单 ，点击导入，将令牌文件导入



8.2 令牌绑定

启用令牌的第二步，就是把令牌序列号与用户绑定。编辑用户，在动态口令卡下拉选择令牌，点击确实即可



9 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。