



# **Array SSL VPN 部署配置手册**

**适用于阿里云环境（包括金融云、政务云等行业云等）**

---

**版本变更记录:**

时间	版本	说明	修改人
2015年9月7日	V1.0	文档创建	保杭, Array
2015年9月9日	V1.5	文档修改	Array
2015年9月22日	V1.7	文档修改	Array
2016年1月8日	V1.8	文档修改	Array
2016年8月16日	V2.0	文档更新	Array
2018年1月9日	V2.2	文档更新	Array

**适用性声明:**

本文档仅适用于阿里云 Array SSL VPN 部署及配置

# 目录

<b>一. Array SSL VPN 组网模式</b> .....	<b>1</b>
<b>1.1 专用网络 VPC 环境</b> .....	<b>1</b>
1.1.1 公网 SLB+VPC 组网模式.....	1
1.1.2 VPN 挂载弹性 IP 模式.....	1
<b>1.2 经典网络环境</b> .....	<b>2</b>
1.2.1 公网 SLB 映射.....	2
1.2.2 VPN 直接使用公网 IP.....	2
<b>二. 阿里云 Array SSL VPN 创建与访问</b> .....	<b>3</b>
<b>2.1 部署 Array SSL VPN</b> .....	<b>3</b>
2.1.1 测试用户部署 Array SSL VPN.....	4
2.1.2 直接购买用户部署 Array SSL VPN.....	5
<b>2.2 利用现有的 ECS 创建 Array SSL VPN</b> .....	<b>7</b>
<b>2.3 管理 Array SSLVPN</b> .....	<b>9</b>
2.3.1 登录指导、管理员账号密码修改.....	9
<b>三. Array SSL VPN 常用配置维护</b> .....	<b>12</b>
<b>3.1 License 申请与导入</b> .....	<b>12</b>
<b>3.2 SSLVPN 虚拟站点建立</b> .....	<b>14</b>
<b>3.3 本地数据库认证建立</b> .....	<b>15</b>
<b>3.4 SSLVPN 建立</b> .....	<b>16</b>
<b>3.5 角色的建立</b> .....	<b>19</b>
<b>3.6 添加本地用户账号</b> .....	<b>21</b>
<b>3.7 登录 VPN 系统</b> .....	<b>21</b>
<b>3.8 VPN 账号权限配置</b> .....	<b>22</b>
<b>3.9 登陆页面图标和登陆信息更改</b> .....	<b>23</b>
<b>3.10 SSLVPN 连接方式</b> .....	<b>23</b>
<b>四. Array SSL VPN 双因素配置</b> .....	<b>24</b>
<b>4.1 动态码获取与绑定</b> .....	<b>25</b>
4.1.1 手机端应用获取.....	25

---

4.1.2 绑定过程.....	25
4.1.3 密码获取.....	26
4.1.4 解除绑定.....	27
<b>五. Array SSL VPN 账户硬件 ID 绑定 .....</b>	<b>28</b>

# 一. Array SSL VPN 组网模式

目前 Array SSLVPN 有**两种**组网模式。

专用网络 VPC : 公网 SLB+VPC 组网模式**或者** VPN 挂载 EIP 模式

经典网络 : 公网 SLB+经典网络组网模式**或者**标准经典网络组网模式

## 1.1 专用网络 VPC 环境

### 1.1.1 公网 SLB+VPC 组网模式

此种模式是 VPC 之外挂载 SLB , 通过 SLB 作为 VPN 的外网访问接入方式。

首先需要在控制台购买 SLB , 然后后面挂载虚拟 VPN。并且开通 443 和 8888 端口 ( **截图看不清楚** )



### 1.1.2 VPN 挂载弹性 IP 模式

为您的 VPN 挂载弹性公网 IP。并且需要提交工单需要开通 443 和 8888 端口访问权限 ( 金融云用户需要提交 )。之后就可以通过外网地址进行登录。

## 1.2 经典网络环境

### 1.2.1 公网 SLB 映射

此种模式是使用经典网络的公网 SLB 将 VPN 服务端口映射到公网。

首先需要在控制台购买 SLB，然后后面挂载虚拟 VPN。并且开通 443 和 8888 端口（截图看不清楚）



### 1.2.2 VPN 直接使用公网 IP

直接使用公网 IP。并且需要提交工单需要开通 443 和 8888 端口访问权限（仅金融云用户需要提交）。之后就可以通过外网地址进行登录。

## 二. 阿里云 Array SSL VPN 创建与访问

本章节主要是针对阿里云客户对 Array SSL VPN 的生成进行创建和初始配置。具体步骤如下：

### 2.1 部署 Array SSL VPN

阿里云客户首先需要创建一个 ECS 并且加载 Array SSL VPN 的镜像。

#### Array SSL VPN 需要的 ECS 推荐配置

CPU : 2 核 ( 推荐 )

内存 : 4GB ( 推荐 )

网络类型 : 专有网路或者经典网络

带宽 : 选择 0M 需要在公网 SLB 开通 443 ( 登录 VPN ) 端口 和 8888 ( 管理 VPN ) 端口

存储 : 默认存储

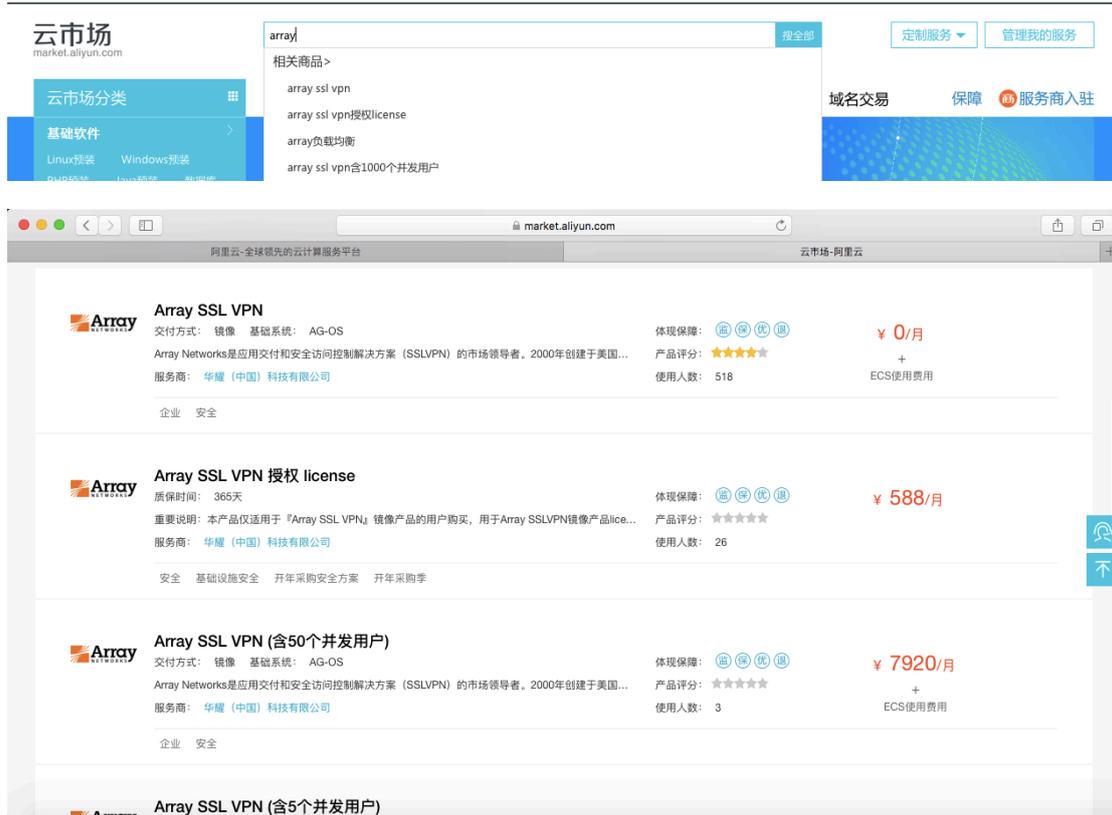
**注 : 1、内存必须等于大于 2G。( 不然 , VPN 服务无法启动 )**

**2、在金融云 ( 含金融和微金融专区 ) 公网带宽必须选 0Mbps。( 不然 , VPN 的 443 端口会侦听在公网 IP 上 , 而金融云又限制不能从互联网直接访问公网 IP。 )**

首先进入阿里云首页, 进入云市场。



在搜索栏中搜索 array



可以看到有几种类型的镜像，含并发与不合并发镜像。

PS：直接购买 Array SSLVPN 使用可以直接选择含并发镜像。若想先进行测试请选择不合并发镜像（0元/月）。

## 2.1.1 测试用户部署 Array SSL VPN

进入 Array SSLVPN 购买页面：



<https://market.aliyun.com/products/56812015/cmjj006220.html?spm=5176.73000>

[5.0.0.nB6ZRS](#)



选择测试地域，注意选择 ECS 配置，推荐是 2 核 4G。由于是进行 SSL VPN 测试，推荐选择按量方式，这个根据用户实际测试时间定，Array 发送至用户的测试 license 是 30 天有效期（**测试 license 申请请看手册 3.1 章节介绍**），最后点击立即购买。



## 2.1.2 直接购买用户部署 Array SSL VPN

根据用户实际并发要求，选择含并发镜像，进入购买页面：





选择使用地域，注意选择 ECS 配置，推荐是 2 核 4G。实际购买使用，推荐选择包月方式，优惠力度更大。如果是短时间使用可以选择按量方式。最后点击立即购买。

PS :并发扩增需求 ,只适用于通过 Array SSLVPN 授权 license 页面购买的许可 ,举个例子，如果某用户实际需求是 10 并发，阿里云市场并没有包含 10 并发的 SSLVPN 专有镜像，这个时候首先部署 0 元的 SSLVPN 镜像，然后进入 Array SSLVPN 授权 license 页面去购买《基础包 A：包含 5 个并发用户+可选配置：每新增五个并发用户》，适用于包年用户（半年的倍数）。

购买成功后，请务必第一时间联系 Array 公司阿里云支持团队：

13918112418（袁先生）或 18511418928（姜小姐）

支持邮箱：aliyun@arraynetworks.com.cn

确认后，我们将第一时间帮您完成新 license 的正式签发工作。



<https://market.aliyun.com/products/56812015/cmfw007482.html?spm=5176.7300>

[05.0.0.nB6ZRS](#)



举例：用户需求购买 15 并发一年：首先购买含 5 并发用户镜像一年，同时购买两次“可选配置：每新增 5 个并发用户数”一年。

## 2.2 利用现有的 ECS 创建 Array SSL VPN

先将此 ECS 停止，点击管理：

实例ID/名称	监控	所在可用区	IP地址	状态(全部)	网络类型(全部)	配置	专有网络属性	付费方式(全部)	操作
i-23rnukto6 iZ23rnukto6Z		华东 1 可用区 C	10.162.87.84 (内)	<b>已停止</b>	经典网络	CPU: 1核 内存: 2048 MB 0Mbps		按量 16-08-17 20:44 创建	<b>管理</b> 更多 ▾

共有1条，每页显示：20条

在配置信息中，点击更换系统盘：

iZ23rnukto6Z
刷新 启动 释放设置

**基本信息** 连接管理终端... 更多 ▾

ID: i-23rnukto6

所在可用区: 华东 1 可用区 C

名称: iZ23rnukto6Z

描述:

地域: 华东 1

实例规格: ecs.s1.small

实例规格族: 标准型 s1

镜像ID: ubuntu1404\_64\_40G\_cloudinit\_20...

标签:

**配置信息** 更换系统盘 更多 ▾

CPU: 1核

网络类型: 经典网络

磁盘: 1

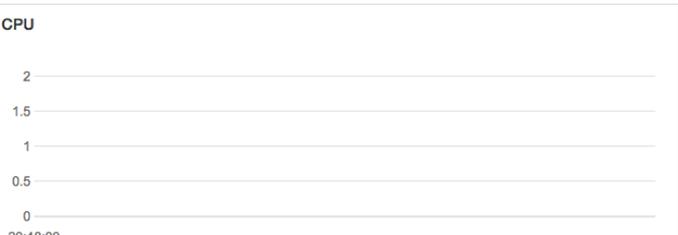
快照: 0

镜像: ubuntu1404\_64\_40G\_cloudi...

状态: **已停止**

**监控信息** 设置报警规则 2016-08-17 19:50 - 2016-08-17 20:50

CPU



出现提示框，更换系统后，原来系统内的 OS 和数据会被全部清除，请提前做好数据备份工作。

点击确定，更换系统盘。

## 更换系统盘



ECS实例更换系统盘后，磁盘ID会变更，原系统盘会被释放。

请注意：

1. 您原系统盘的用户快照会保留，自动快照则根据您该系统盘属性值“自动快照是否随磁盘释放”的选项来判断是否保留或随磁盘删除；您可以进入磁盘列表点击“修改属性”查看或修改属性值。
2. 自动快照策略将失效，需要重新设置。
3. 您在操作前做好相关备份，以免数据丢失给你造成损失。

确定，更换系统盘

取消

在镜像市场的云安全市场选择 Array SSLVPN，点击同意并使用。（包年包月的 ECS ECS 替换镜像只会显示含并发用户的 SSLVPN 镜像）

## 镜像市场[华东 1]



如需选购镜像包月套餐，请点击镜像名称购买，访问 [云市场](#) 发现更多软件和优惠！

运行环境

管理与监控

建站系统

应用开发

数据库

服务器软件

企业软件

**云安全市场**

已购买的镜像

已订阅的镜像

array



### Array SSL VPN

V1.8

¥0.00 /时

来源：华耀（中国）科技有限公司

ArrayNetworks公司的vxAG产品，提供随时随地基于浏览器的安...

已购买：1个 在使用中：0个 剩余可用：1个

同意并使用

同意《镜像使用协议》

### Array SSL VPN（含1000个并发用户）

9.4

¥145.00 /时

来源：华耀（中国）科技有限公司

ArrayNetworks公司的vxAG产品，提供随时随地基于浏览器的安...

同意并使用

同意《镜像使用协议》

### Array SSL VPN（含100个并发用户）

9.4

¥18.00 /时

来源：华耀（中国）科技有限公司

ArrayNetworks公司的vxAG产品，提供随时随地基于浏览器的安...

同意并使用

同意《镜像使用协议》

### Array SSL VPN（含50个并发用户）

9.4

¥11.00 /时

来源：华耀（中国）科技有限公司

ArrayNetworks公司的vxAG产品，提供随时随地基于浏览器的安...

同意并使用

同意《镜像使用协议》

上一页

1

2

下一页

最后点击同意并使用即可，并点击更换（版本选择以最新版本为准，下拉框最顶端为最新版本）。

镜像名称: Array SSL VPN V1.8  
[重新选择镜像](#)

系统盘: 普通云盘 40 GB 200~500 IOPS 系统盘设备名: /dev/xvda  
[如何选择 SSD云盘 / 高效云盘 / 普通云盘, 请看 详细说明>>](#)

登录名: root

登录密码:  8 - 30 个字符, 且同时包含三项 ( 大写字母, 小写字母, 数字和特殊符号 )

确认密码:

镜像费用: ¥0.00 /时  
配置费用: ¥0.44 /时  
 《云服务器 ECS 服务条款》  
[确定更换](#)

( 此处应该也可以选择按量计费的镜像, 需要解释清楚 )

## 2.3 管理 Array SSLVPN

使用浏览器登录 `https:// array 设备 VPN 外网 IP : 8888`

例: `https:// 120.26.116.10:8888`

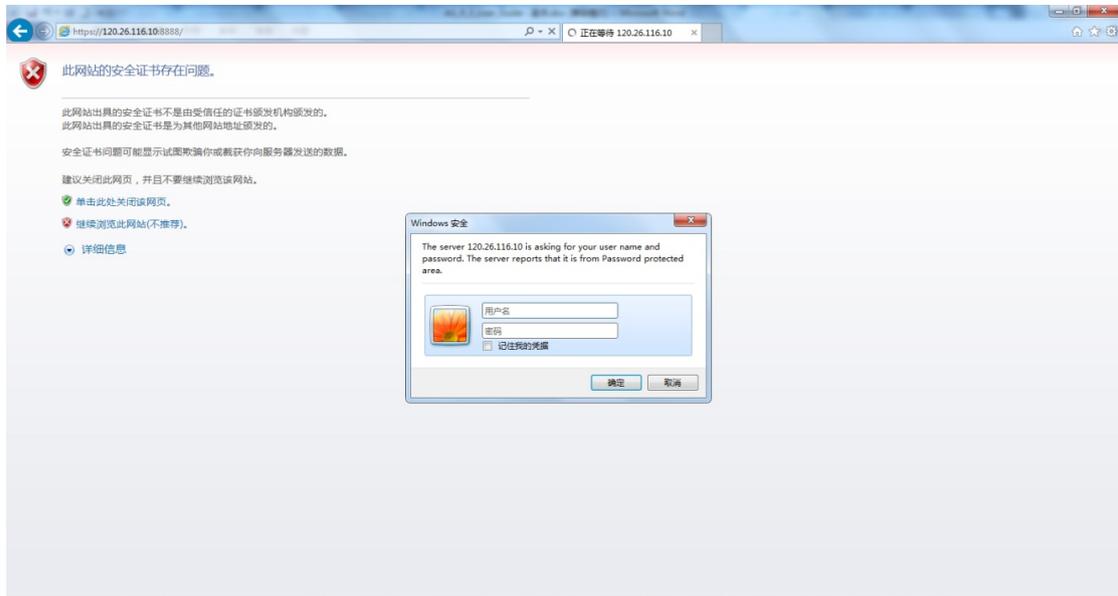
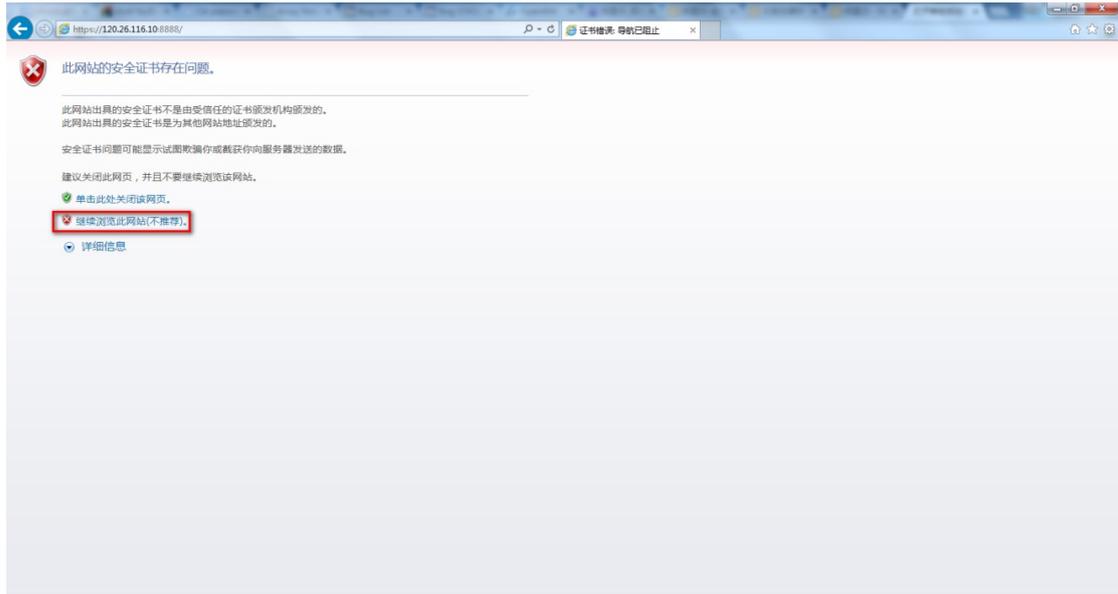
需要说明:

如果客户使用的是 SLB ,则需要在 SLB 开通 443( 登录 VPN )端口 和 8888

( 管理 VPN 的 Web 控制台 ) 端口

### 2.3.1 登录指导、管理员账号密码修改

在浏览器输入地址截图如下



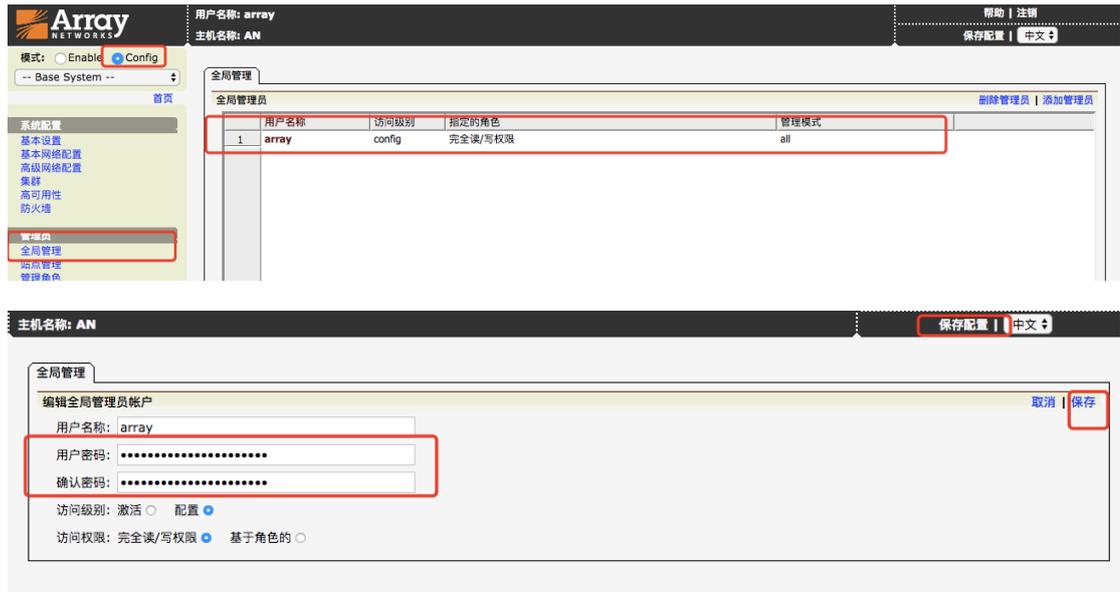
## 管理员用户名和密码

Array SSL VPN 设备默认管理员账号： array 密码：admin

Enable 密码：默认未设置，直接点击 login 即进入 web 控制台。

管理员密码修改：

全局模式下 config 模式下-全局管理-双击管理员账户



修改完密码后点击保存，最后点击保存配置，将当前配置存盘

需要注意的是，配置模式只允许单管理员登陆，万一出现管理员在配置模式时非正常退出，导致再次登陆进入配置模式报错：

系统提示信息：

Administrator "array" is in config mode.  
Access denied!!!!

取消 好

必须在访问控制中重置管理员账户 config 模式：

系统管理-访问控制-config 模式：重设到初始值



Enable 密码设置：

系统管理-访问控制-新的 Enable 密码



## 三. Array SSL VPN 常用配置维护

### 3.1 License 申请与导入

部署 0 元镜像的试用用户需要提前申请测试 license，**购买含并发用户镜像** **无需申请**。申请方式如下：

在登录界面找到序列号，发邮件联系厂商可申请 15 天临时 license 供测试使用。

申请测试 license 请发送至以下邮件：

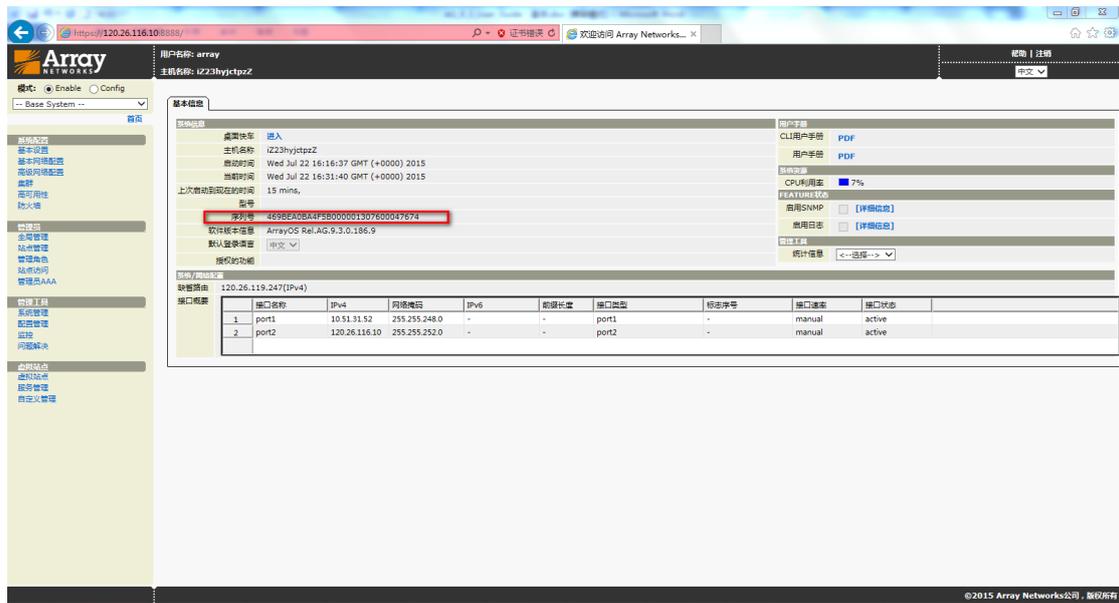
[pujl@arraynetworks.com.cn](mailto:pujl@arraynetworks.com.cn)

或者联系钉钉：18616026366

发送测试 license 申请请备注公司名、联系人姓名和手机号码，并把实际测试并发用户写明，若未写明一律按照 5 个并发数申请。

注：如果没有 license，服务将不可用。

序列号显示位置：

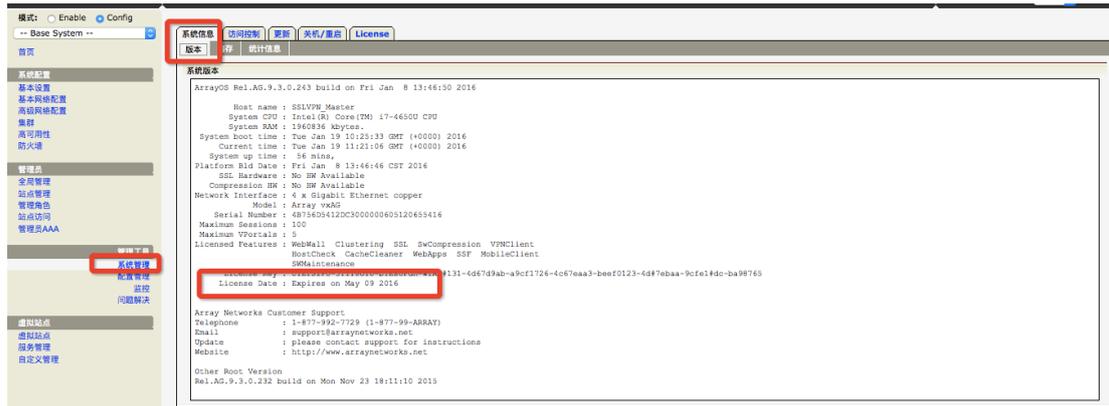


导入 license，注意需要带校验导入 license。



导入成功后请立即重启虚拟机，等管理页面能够正常登录后，继续后续操作。

查看 license 到期时间：



注意：购买含并发镜像无需考虑 license 许可问题，该步骤可以忽略。

### 3.2 SSLVPN 虚拟站点建立

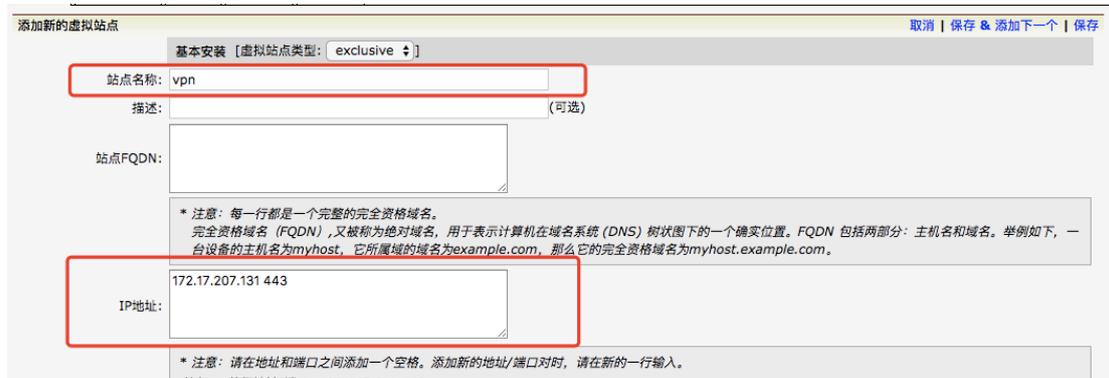
首先我们需要创建一个虚拟站点，进入全局模式 config 模式下->虚拟站点->添加站点：



站点名称：自定义

IP 地址：VPC 环境填写私有地址，默认端口 443

经典网络环境填写公网地址，默认端口 443



生成自签发证书，证书信息填写自定义即可（该服务器证书在浏览器中未受信，若有受信证书可以直接在创建虚拟站点时导入）



填写完以上信息后点击保存。

这样我们就能在左上角下拉菜单中看到我们新创建的虚拟站点了。选中虚拟站点可以进入站点模式下配置相关的 VPN 配置。

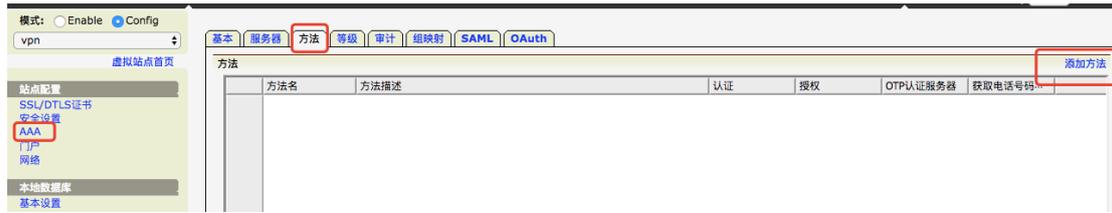


### 3.3 本地数据库认证建立

array 管理员登陆->切换到vpn站点->AAA->服务器->本地数据库->启用本地数据服务器->应用修改



AAA->方法->添加方法



方法名：自定义

认证选择 vpn（默认数据库启用后，本地数据库名称和站点名称相同）



最后点击保存。

以上为本地数据库认证启用方式，如果有其他认证方式要求，请咨询钉钉号 18616026366。

### 3.4 SSLVPN 建立

**SSLVPN 访问区域配置：**

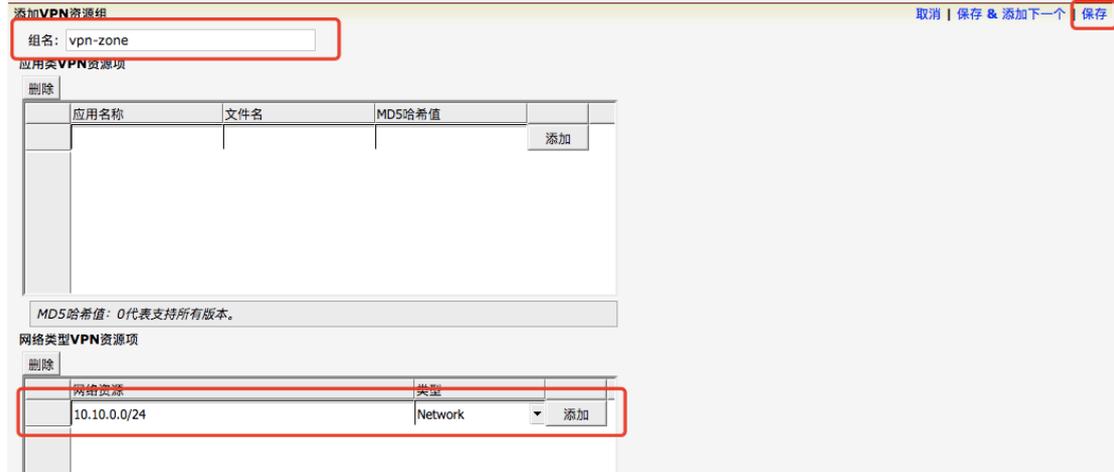
array 用户登陆->切换到 vpn 站点->Config 模式->VPN->通用设置->VPN 资源->添加



资源：自定义

网络类型 VPN 资源项：填写需要通过 SSLVPN 接入后管理的 IP 地址或 IP 地址段，点击添加，可以多次添加。

最后点击保存。



### SSLVPN 客户端分配地址池配置：

VPN->通用设置->Netpool->增加 Netpool



Netpool 名称：自定义

启用 NAT 选项说明：勾选启用 nat 后，用户端分配的 netpool 地址经过 sslvpn 会 nat 成站点服务 ip（即 ECS 内部地址）；

不勾选代表使用路由模式，源地址为 VPN 实际分配给客户端的 netpool 地址，为了支持路由模式正常工作，必须在内部指定一条 vpn 分配地址池的目的路由。

经典网络模式只支持 NAT 模式

VPC 网络模式支持 NAT 模式和路由模式

请根据实际网络环境挑选部署模式

最后点击保存。



双击新建的 netpool 名称

VPN资源										
Netpool										
NETPOOL <span style="float: right;">删除Netpool   增加Netpool</span>										
	Netpool名称	Web客户端模式	启用启动模式...	自动启动	保持连接	NAT	客户端子网	保持活动时间...	Standalone托...	托盘图标
1	netpool	activex	X			X		30	X	X

在动态 IP 地址范围中填写对应的地址区间并点击添加（此处我用了 192.168.100.0/24 这个段地址）

动态IP地址范围			
起始IP地址	结束IP地址	HA单元名称	
192.168.100.1	192.168.100.254	<--选择-->	添加

VPC 环境中 SSLVPN 分配地址池路由的创建（在不勾选启用 nat 需要添加）  
在指定的 VPC 路由器中添加路由，下一条选择 SSLVPN 的 ECS 实例



\*目标网段:

必须是一个合法的CIDR或IP地址，例如：  
192.168.0.0/24 或 192.168.0.1

下一跳类型:

\*下一跳ECS实例:

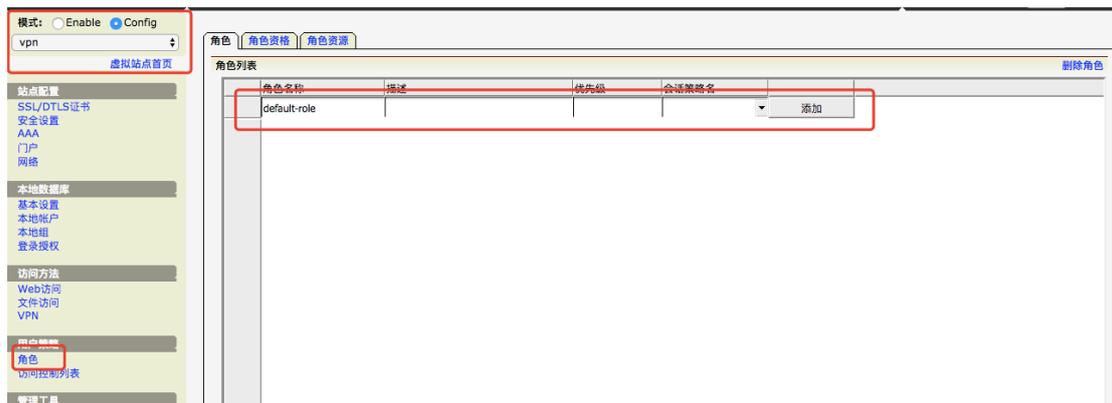
最后启用 SSLVPN 功能，VPN->SSLVPN>勾选启用 VPN->应用修改，



### 3.5 角色的建立

在之前我们已经建立了认证, SSLVPN 的资源 and 分配地址段, 我们需要将这些元素联系起来, 通过创建角色完成我们最后的配置步骤:

array 用户登陆->切换到 vpn 站点->Config 模式->角色->填写角色名称->添加



在角色中至少要定义一个角色资格

角色资格->添加

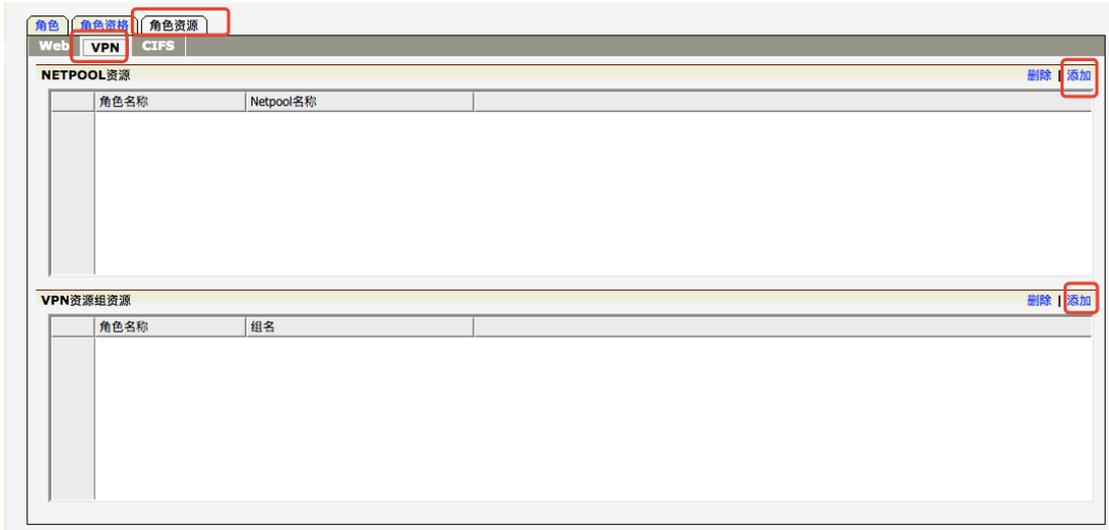


资格名称: 自定义



最后关联角色的 VPN 资源

角色资源->VPN->NETPOOL 资源->添加

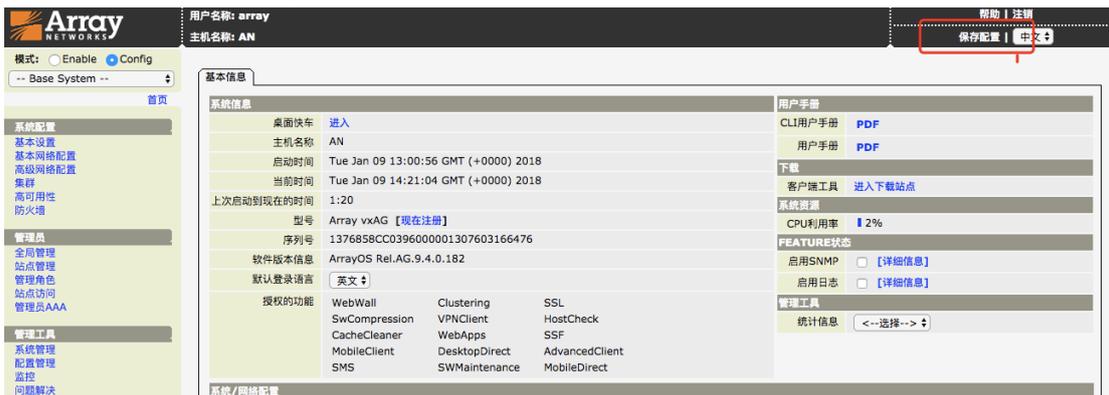


### VPN 资源组资源->添加



以上我们已经完整的定义了整个 SSLVPN 的配置。最后我们要把配置存盘（这点非常重要，否则重启配置会丢失）

全局模式下->Config 模式->保存配置->保存全局和所有虚拟站点配置



### 3.6 添加本地用户账号

以上我们已经配置完了 SSLVPN 服务，接下来我们通过添加账户就可以开始使用 Array SSLVPN 业务了。

登录 VPN 设备后，创建需要使用的 VPN 账户：

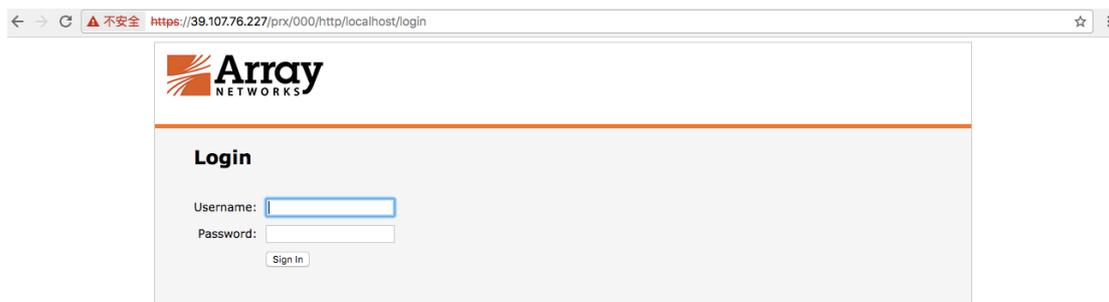
array 用户登陆->切换到 vpn 站点->Config 模式->本地数据库->本地账户->添加



### 3.7 登录 VPN 系统

添加完用户浏览器登陆 https://ecs 主机外网 ip 到用户登陆界面。注意：同样需要在 SLB 上映射 443 端口。才可以通过外网进行访问登录。

例：https://39.107.76.227



### 3.8 VPN 账号权限配置

默认情况下，用户正常登录后，能够访问 VPN 可访问区域网段中的所有应用，如果需要给具体的某个用户定义 ACL，按如下方式定义：

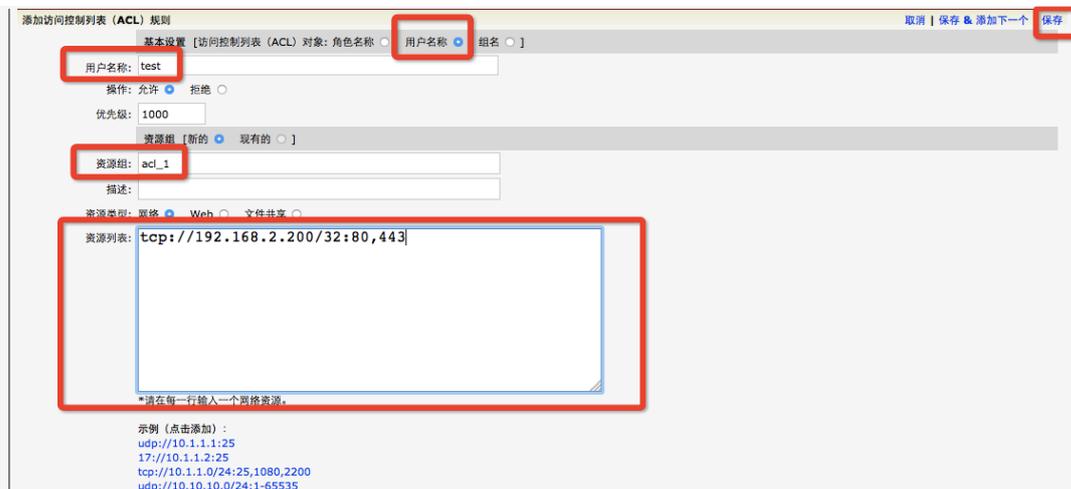
array 用户登陆->切换到 vpn 站点->Config 模式->用户策略->访问控制列表->

基本 ACL->ACL 规则

添加具体明细 ACL：



访问控制列表选基于用户名的方式，选择本地数据库中具体的用户名，资源组名称随机定义，资源列表根据以下示例添加。添加完成后，默认行为是 deny，以下截图是针对 test 这个用户只开放 192.168.2.200 这个地址的 80 和 443 端口。注意：针对当前登录用户更改权限后，需要让此用户注销重新登录，才能分配到新更改后的权限。（若用户量比较大，可以选择基于本地组分配 ACL 资源）



### 3.9 登陆页面图标和登陆信息更改

在站点模式下，以下界面标注处能够更改登陆页面语言和 Logo 图标：



以下界面标注处可以修改登陆页面的登陆信息和欢迎页面的登陆标题和信息



### 3.10 SSLVPN 连接方式

请详细阅读 [Array SSL VPN 客户端使用手册](#)

## 四. Array SSL VPN 双因素配置

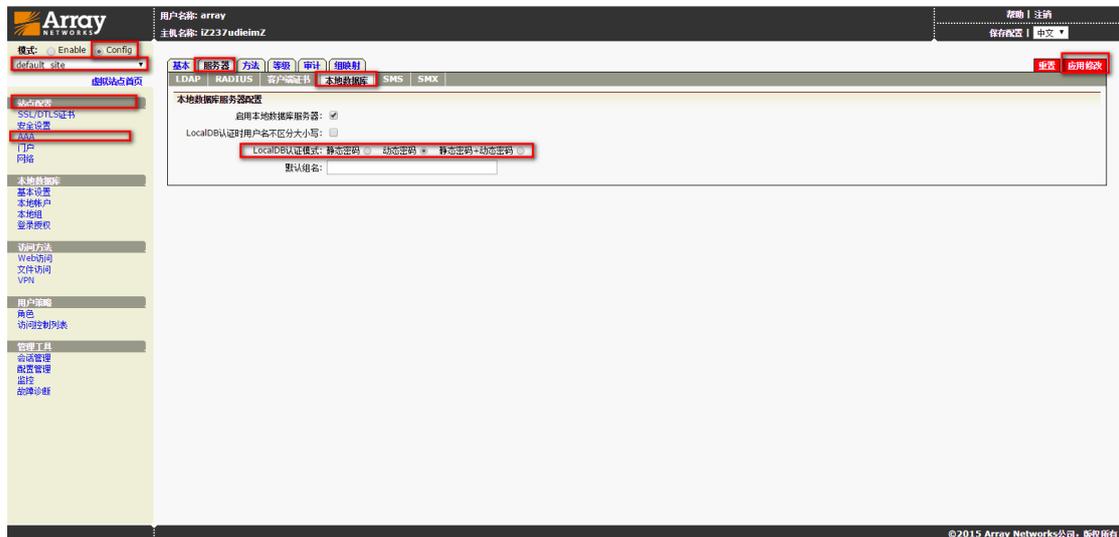
Array SSL VPN 提供三种密码认证方式：**静态密码，动态密码，静态密码 + 动态密码。**

**静态密码**：最基本的认证模式，登陆密码为添加用户时设置的密码。

**动态密码**：利用 Array OTP 手机应用与站点及用户绑定后生成的 6 位数动态密码登陆

**静态密码 + 动态密码**：密码格式为静态密码与动态密码连接（例：静态密码为 secret，获取当前动态密码为 123456，则登陆密码为 secret123456）。

**配置**：array 用户登陆->切换到 default\_site->Config 模式->站点配置->AAA->服务器->本地数据库->LocalDB 认证模式->应用修改



## 4.1 动态码获取与绑定

### 4.1.1 手机端应用获取

IOS 系统在 Apple Store 搜索 MotionProOTP 应用安装。

Android 系统可在 360 手机助手或小米应用商城下载 MotionProOTP 应用。

链接如下：

[http://zhushou.360.cn/detail/index/soft\\_id/3083541?recrefer=SE\\_D\\_](http://zhushou.360.cn/detail/index/soft_id/3083541?recrefer=SE_D_)

[MotionProOTP](#)

<http://app.xiaomi.com/details?id=com.arraynetworks.authentication>

[&ref=search](#)

### 4.1.2 绑定过程

以 Android 系统为例打开后如下图所示，iOS 系统过程基本相同。



服务器地址：为前文所说 VPN 登陆界面 ( <https://服务器地址> ) 中的服务器地址。

端口：默认为 443

用户名：该用户登陆 VPN 时的用户名。

密码：添加用户时设置的密码，即静态密码。

### 4.1.3 密码获取

绑定成功后如下图所示，密码为 30S 更新一次。



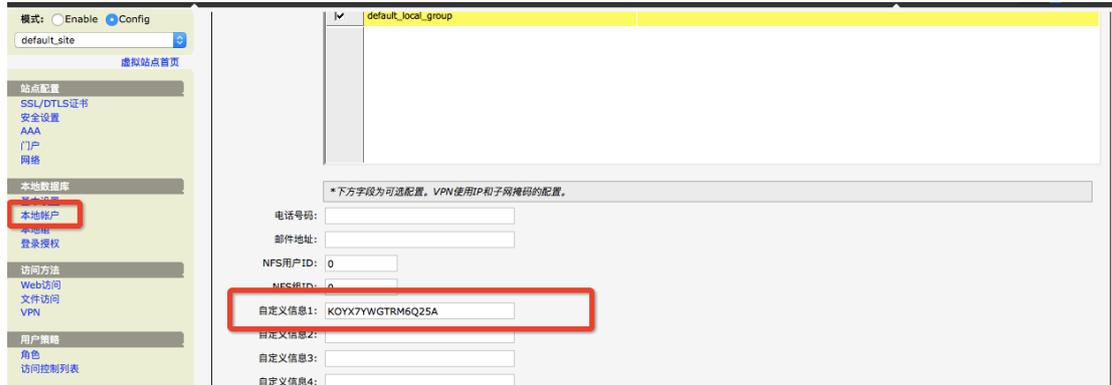
#### 4.1.4 解除绑定

客户端解除绑定：



VPN 管理端强制解除绑定：

在本地账户中选择对应的账户，将自定义信息 1 中的字符串删除即可。



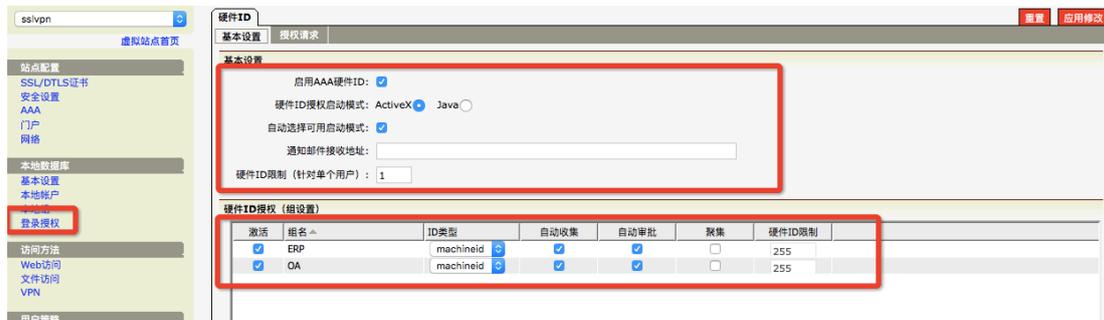
## 五. Array SSL VPN 账户硬件 ID 绑定

需要实现用户认证账户与登录终端设备的绑定。

PS：不能和双因素认证同时使用（前面章节介绍的手机令牌方式）

首先进入站点模式下，点击本地数据库中登录授权：

设置前先建立好本地组，推荐方式 machineid 和 macany。



必须开启自动收集，自动审批可根据实际情况开启或不开启。

若开启自动审批功能，单个账户允许的终端绑定数量由硬件 ID 限制的数量决定。

可以在授权请求中看到账户和终端绑定的授权信息：



若自动审批功能不开启，默认状态是 deny，需要管理员进行放行。



deny 状态下会提示：



解除账户的终端绑定，选中对应账户绑定条目后点击拒绝即可。

