



绿盟堡垒机云服务(vOSMS)

腾讯云快速实践指南



文档版本： V5.6.10 (2018-06-27)

© 2018 绿盟科技

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属北京神州绿盟科技有限公司（简称绿盟科技）所有，受到有关产权及版权法保护。任何个人、机构未经绿盟科技的书面授权许可，不得以任何方式复制或引用本文的任何片断。

前言.....	1
1 概述.....	4
1.1 服务概述	4
1.2 快速使用指南概述	5
2 示例介绍.....	6
2.1 原始虚拟网络内的典型拓扑结构.....	6
2.2 使用堡垒机后的拓扑结构.....	7
2.3 示例说明	8
3 部署前准备工作.....	10
3.1 准备云主机.....	10
3.2 证书获取方法.....	10
4 环境部署.....	11
4.1 网络规划	11
4.2 配置虚拟网络.....	11
4.3 配置子网	12
4.4 配置安全组.....	13
4.4.2 FrontEnd 的安全组	14
4.4.3 BackEnd 的安全组.....	15
4.4.4 OsmsEnd 的安全组.....	15
4.5 创建 Server 实例.....	16
4.6 部署 vOSMS 实例	16
4.6.1 从云市场创建新实例.....	17
4.6.2 从控制台创建新实例.....	18
4.6.3 使用空闲云主机	19
4.7 创建前置机实例.....	19
5 导入许可证和快速配置.....	20
5.1 对 vOSMS 进行管理.....	20
5.2 导入许可证.....	21
5.3 配置字符审计	22
5.4 配置前置机数据库图形审计	26

5.5 配置短信认证.....	29
6 其他配置说明	32
6.1 初始用户	32
6.2 端口说明	32
6.3 更多配置方式.....	33

文档范围

本文详细介绍了绿盟堡垒机云服务(vOSMS)在腾讯云上的快速部署过程。

读者对象

本文档主要适用于以下读者：

- 期望了解在腾讯云部署的部署过程的用户
- 系统管理员
- 网络管理员

本文假设您对下面的知识有一定的了解：

- 系统管理
- Linux、Windows 操作系统
- Internet 协议
- TCP/IP 协议
- 腾讯云相关知识，包括但不限于如下：

内容	链接
云服务器/云主机	https://cloud.tencent.com/document/product/215/8116
私有网络 VPC	https://cloud.tencent.com/document/product/215/8113
子网	https://cloud.tencent.com/document/product/215/8114
路由器	https://cloud.tencent.com/document/product/215/8115
安全组	https://cloud.tencent.com/document/product/215/8117
负载均衡 LB	https://cloud.tencent.com/document/product/214/6149

内容概述

标题	概述
概述	介绍服务概况，说明本文的目的和适用范围

标题	概述
示例介绍	介绍部署虚拟本服务前后在腾讯云上的拓扑变化，概况介绍本示例的主要信息
部署前准备工作	确定部署前需要获取的内容
环境部署	从创建 VPC 开始，到完成所有实例的配置
导入许可证和快速配置	启用虚拟堡垒机

格式约定

符号	说明
粗体字	菜单、命令和关键字
<i>斜体字</i>	文档名、变量
 说明	对描述内容的补充和引用信息
 提示	使用设备时的技巧和建议
 注意	需要特别注意的事项和重要信息
 警告	有可能造成人身伤害的警告信息
【XXX】	按钮名称的表示方式
A > B	菜单项选择的表示方式

获得帮助

绿盟云

云端安全服务专家，为企业客户提供专业的 SaaS 安全服务。

网站：<https://cloud.nsfocus.com>

绿盟科技官网

可以帮助用户获取最新的网络安全信息和绿盟安全产品信息。

网站: <http://www.nsfocus.com.cn>

售后服务

提供全国范围内的服务热线,可以帮助用户解决在使用绿盟科技产品和服务过程中遇到的各种问题和困难。

网站: <http://www.nsfocus.com.cn/operations/>

软件升级

在进行产品使用培训后,可以帮助用户自助进行产品的升级操作。

网站: <http://update.nsfocus.com/>

产品生命周期公告

可以帮助用户获取已经停止的服务信息和已经下线的产品信息。

网站: <http://www.nsfocus.com.cn/support/>

1 概述

目前，随着企事业单位 IT 系统的不断发展，网络规模和设备数量迅速扩大，日趋复杂的 IT 系统与不同背景的运维人员的行为给信息系统安全带来较大风险。绿盟堡垒机云服务(vOSMS)给我们提供一套多方位的运维管理解决方案，使得管理人员可以全面对各种资源（包括网络设备、主机、安全设备和数据库）进行集中帐号管理、细粒度的权限管理和访问审计，帮助企业提升内部控制风险的水平。

本章主要包含以下内容：

功能	描述
服务概述	简单介绍服务场景。
快速使用指南概述	简单介绍本指南的内容。

1.1 服务概述

绿盟堡垒机云服务(vOSMS)通过一个集中管控平台整合企业设备的运维行为管理，使运维操作集中可视化，解决多种设备类型带来的管理问题。

服务有如下几个特点：

- 和公有云深度集成
可以在国内主流的公有云上直接使用，快速部署，能解决当前有“云上”业务的企业客户有业务、没安全的尴尬局面。
- 集中账号管理
建立基于唯一身份标识的全局实名制管理，支持统一账号管理策略，实现与各服务器、网络设备等无缝连接，集中管理主账号（普通用户）、从账号（目标设备系统账号）及相关属性。
- 集中访问控制
通过集中统一的访问控制和细粒度的命令级授权策略，确保用户拥有的权限是完成任务所需的最小权限，实现集中有序的运维操作管理，防止非法、越权访问事件发生。
- 集中安全审计

基于唯一身份标识，通过对用户从登录到退出的全程操作行为审计，监控用户对被管理设备的所有敏感关键操作，提供分级告警，聚焦关键事件，实现对安全事件及时预警发现、准确可查。

1.2 快速使用指南概述

本指南主要是指导使用者如何在腾讯云上快速使用绿盟堡垒机云服务(vOSMS)，通过一个具体示例的讲解，期望达到的目标是：

- 了解在部署 vOSMS 前需要准备哪些内容
- 了解如何快速部署一套多方位云平台运维管理系统



注意

本指南所涉及内容只适用于于腾讯云中国区域，如果需要在腾讯云其他区域上使用，请联系我们获取更多信息

2 示例介绍

介绍示例部署在腾讯云上原始逻辑结构、数据流向，以及使用本服务后的逻辑结构及数据流量的变化

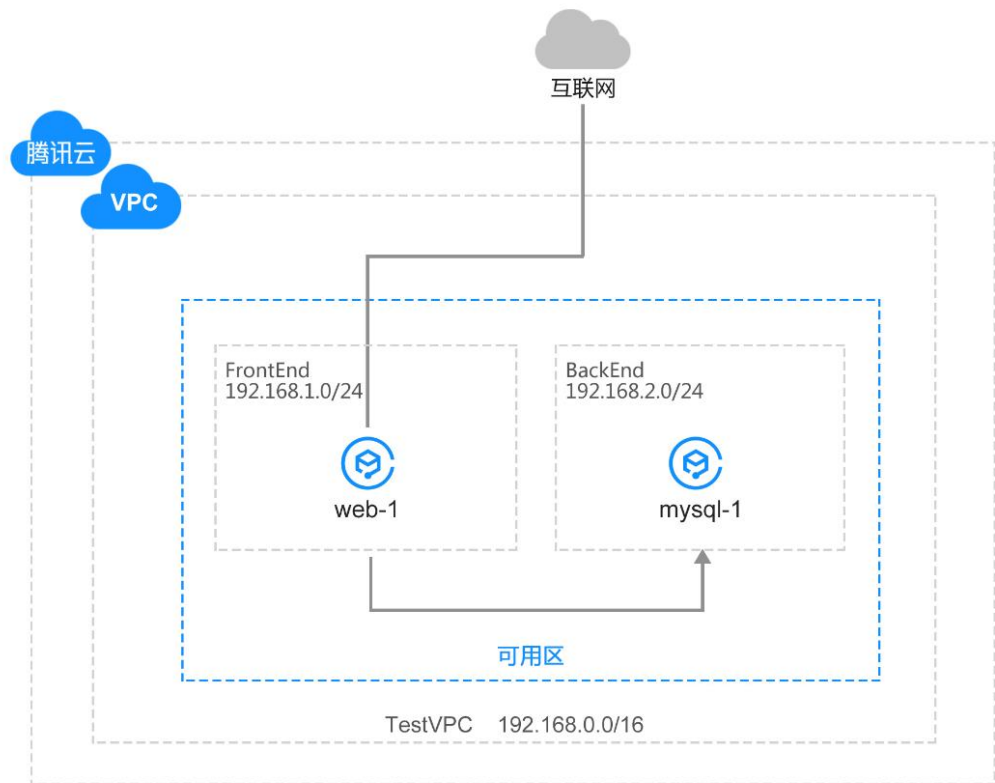
本章主要包含以下内容：

功能	描述
典型的原始部署结构	部署结构及数据流向。
使用本服务后的典型结构	部署结构及数据流向的变化。
本指南中的示例概述	示例结构的拓扑及主要实例

2.1 原始虚拟网络内的典型拓扑结构

典型环境主要包括以下部分：

- 包含两个子网，部署 Web Server 的前端子网和部署 DB Server 的后端子网。



数据流向为:

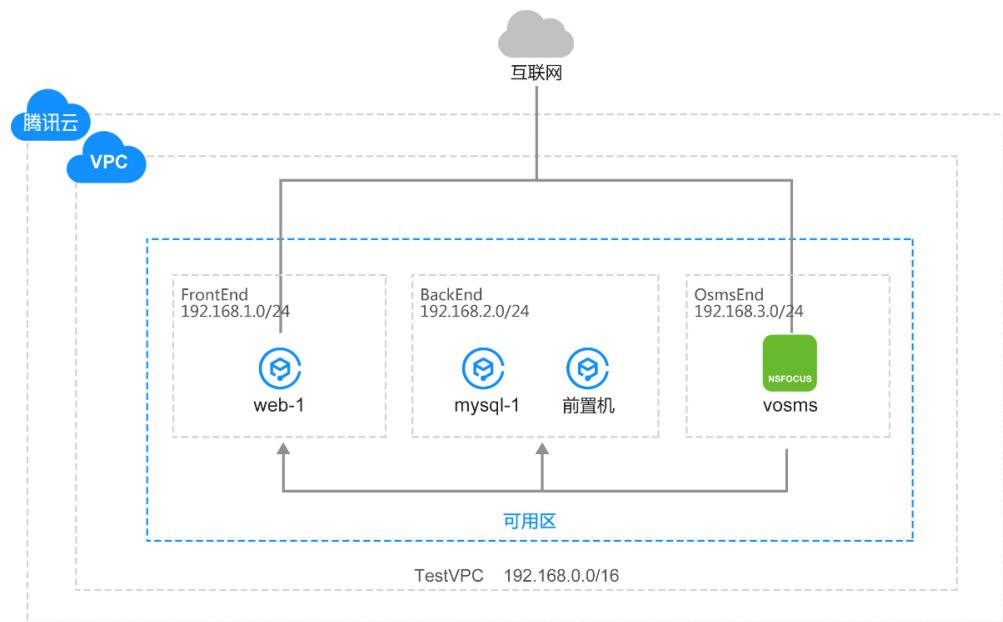
- 可以直接通过 Internet 访问部署在前端子网的 web 服务器 22 端口 (用于服务器后台访问), 80 端口 (用于最终客户的 web 网站访问)。
- 只能通过前端子网访问后端子网 mysql 服务器 22 端口 (用于服务器后台访问), 3306 端口 (用于 web 服务器访问 mysql)。
- 后端子网无法直接访问 Internet。

----结束

2.2 使用堡垒机后的拓扑结构

在虚拟网络中增加 vOSMS 后, 拓扑图中的主要元素有

- 包含 3 个子网, 和原始拓扑相比, 增加了部署堡垒机的子网, 定位于运维或研发人员远程对业务系统或数据库进行维护。
- 在 BackEnd 子网部署一台 Windows Server 2008 用于数据库图形化审计。



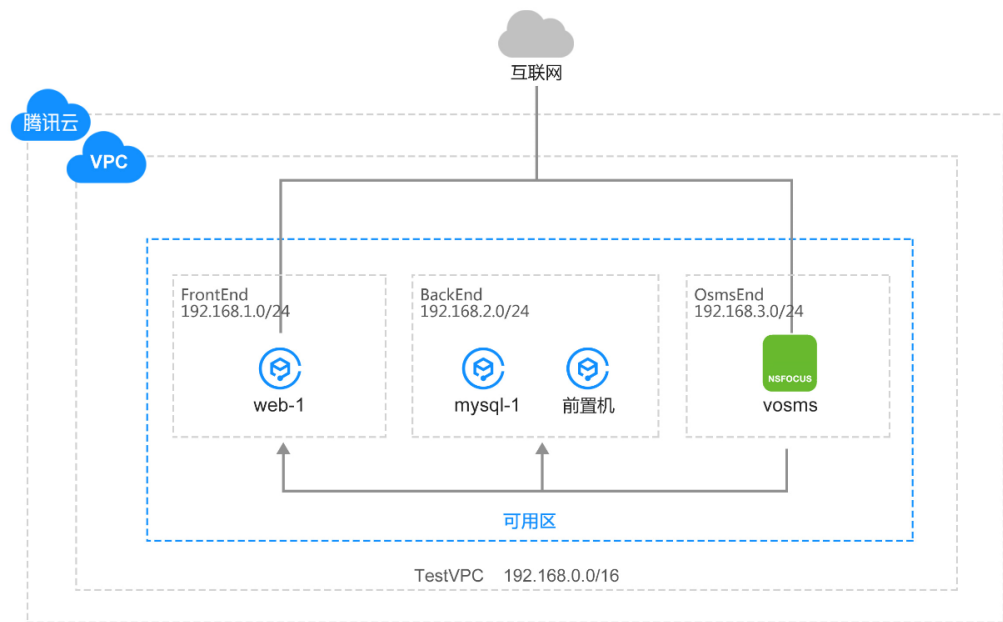
数据流向为：

- 可以直接通过 Internet 访问部署于前端子网的服务器 80 端口。
- 只能通过前端子网访问部署于后端子网服务器的 3306 端口。
- 后端子网无法直接访问 Internet。
- 可以通过 vOSMS 子网访问前端及后端子网服务器的 22 端口。
- 可以通过 vOSMS 子网访问后端子网前置机的 3389 端口。
- 可以直接通过 Internet 访问部署于堡垒子网的堡垒机 22, 443 端口。

----结束

2.3 示例说明

本指南中将会搭建如下示例拓扑，适用于网站常见部署场景。



具体包含:

- 1 个客户的虚拟网络: TestVNet。
- 3 个子网:
 - 用于部署 Web Server 的前端子网 FrontEnd, 关联 NSG-FrontEnd 网络安全组。
 - 用于部署 DB Server 的后端子网 BackEnd, 关联 NSG-BackEnd 网络安全组。
 - 用于部署堡垒机的管理子网 OsmsEnd, 关联 NSG-OsmsEnd 网络安全组。
- 1 台用作 web server 的虚拟机 web-1, 部署在 FrontEnd 子网。
- 1 台用作 mysql 的 VM mysql-1, 部署在 BackEnd 子网。
- 1 台用作数据库图形审计的 VM 前置机, 部署在 BackEnd 子网。
- 1 个用作 vOSMS 的 VM。位于 OsmsEnd 子网, 其中堡垒机网卡具有外网 IP, 用于互联网访问。

----结束

3 部署前准备工作


部署 vOSMS 之前，确认以下一些资源是否已经具备。

所需内容	用途
准备云主机	需要单独准备部署 vOSMS 的云主机，不能与其他系统共用
vOSMS 许可证	需要导入到 vOSMS 的云主机后，才能正常使用

本章主要包含以下内容：

功能	描述
准备云主机	最终用户如何准备前期虚拟资源
证书获取方法	最终用户如何获取这些资源

3.1 准备云主机

 注意	部署 vOSMS 之前最终用户需要单独准备部署 vOSMS 的云主机，不能与其他系统共用
--	--

具体有三种准备方式，详见 4.6 章节，实例规格详见《绿盟堡垒机云服务技术白皮书》的内容。

----结束

3.2 证书获取方法

当您在腾讯云镜像市场下单购买绿盟堡垒机云服务(vOSMS)后，可以联系您的客户经理或绿盟科技销售人员，告诉我们您的购买信息或合同信息，服务开始时间以及其他重要的相关信息，信息确认无误后，我们将会 在 3 个工作日内完成证书生成工作，并将信息反馈给您。

----结束

4 环境部署

本章主要包含以下内容：

功能	描述
配置 VPC	介绍如何配置 VPC
配置子网	介绍如何配置子网
配置网络安全组	介绍如何配置网络安全组
搭建 Web Server 和 DB Server	介绍搭建 Web Server 虚拟机和 MySQL 虚拟机
创建 vOSMS 实例	介绍如何在已有环境中接入堡垒机及配置网络
创建前置机实例	介绍如何创建前置机实例

4.1 网络规划

地域：华北地区

私有网络网段为 192.168.0.0/16

将 vOSMS 部署于子网网段 192.168.3.0/24

将数据库前置机部署于子网网段 192.168.2.0/24

将 Web Server 服务器云主机和 DB Server 服务器云主机分别部署在子网网段 192.168.1.0/24、192.168.2.0/24

4.2 配置虚拟网络

步骤 1 登录 <https://console.cloud.tencent.com/>

步骤 2 单击 “私有网络”

步骤 3 在显示的“私有网络”页面中，点击“创建私有网络”：

步骤 4 在显示的“创建私有网络”弹出框中，在“私有网络名称”中输入 TestVPC；在“网段”中选择 192.168.0.0/16；然后单击“创建 VPC”按钮，如下图所示：



步骤 5 创建子网，这里创建一个网段为“192.168.1.0/24”，名称为 FrontEnd 的交换机。



----结束

4.3 配置子网

根据第三章的拓扑，开始配置子网。此处需要配置三个子网、分别用于堡垒机子网，互联网访问区域的子网和内部子网。

3 个需要创建的子网的主要信息如下表：

子网名称	CIDR	用途说明
FontEnd	192.168.1.0/24	Web Server 前端子网
BackEnd	192.168.2.0/24	MySQL 后端子网
OsmsEnd	192.168.3.0/24	vOSMS 管理子网

该门户仅允许用户在创建 VPC 时创建一个初始子网。对于此方案，必须在创建 VPC 之后创建第二个子网。选择菜单子网，按上表创建成功后如下图所示：

ID/名称 ↓	所属网络	CIDR	可用区	关联路由表
subnet-lowe5scf FrontEnd	vpc-gayn3i14 TestVPC	192.168.1.0/24	北京一区	rtb-9d97dhk7 default
subnet-4dnc5bb1 BackEnd	vpc-gayn3i14 TestVPC	192.168.2.0/24	北京一区	rtb-9d97dhk7 default
subnet-8aphhp6h OsmsEnd	vpc-gayn3i14 TestVPC	192.168.3.0/24	北京一区	rtb-9d97dhk7 default

----结束

4.4 配置安全组

在腾讯云中，安全组是指不同实例所关联的一系列获得批准的（仅“允许”）传入和传出规则。

访问云服务器的菜单 **安全组**，进入安全组管理页面。

创建云主机和负载均衡器的时候，均需要指定安全组，来规定允许出\入的流量规则

每个安全组有两套规则：传入规则和传出规则。传入规则决定了流量如何进入云主机，传出规则可用于对离开实例的流量进行检查。

按照如上规划图，下面几个章节开始创建各安全组（只对安全组入站流量规则进行说明，出站流量无限制）。

1. 分隔 Web 和 DB 服务器之间的流量。
2. 不能从 Internet 访问后端 VM。
3. 允许从 Internet 访问前端 VM 端口 80。
4. 允许从 FrontEnd 子网访问任何 DB 服务器的端口 3306。
5. 允许从 OsmsEnd 子网访问任何前端或后端的 VM 端口 22。
6. 允许从 OsmsEnd 子网访问数据库前置机 VM 端口 3389。
7. 允许从 Internet 访问 vOSMS 的端口 22, 443, 3389, 50018, 50019。



说明

22 用于字符方式访问设备
 443 用于 Apache 监听端口
 3389 用于 RDP 访问设备
 50018 用于 RDP 图形代理
 50019 用于图形日志回放和实时查看

将这些规则组合起来可创建一个与 DMZ 类似的方案，其中后端子网只能接收来自前端子网的 API 通信的传入流量且不能访问 Internet，而前端子网可以与 Internet 通信。

----结束

4.4.2 FrontEnd 的安全组

创建名称为“SG_FrontEnd”的安全组：

新建安全组
✕

模板

名称

所属项目

备注

[显示模板规则](#)

确定
取消

入站规则要点为：

来源	协议	端口	访问	优先级	说明
Internet	TCP	80	允许	1	本例中，将 web server 子网配置为接收提供 HTTP 服务的端口：80。
192.168.3.0/24	TCP	22	允许	1	允许来自 OsmsEnd 的 SSH（22）端口访问

配置完成后如下图：



----结束

4.4.3 BackEnd 的安全组

创建一个名为 “SG-BackEnd” 的安全组，配置方式见 4.3.1 节。

入站规则要点为：

来源	协议	端口	访问	优先级	说明
192.168.3.0/24	TCP	22	允许	1	允许来自 OsmsEnd 的 SSH (22) 端口访问
192.168.3.0/24	TCP	3389	允许	1	允许来自 OsmsEnd 的 RDP(3389) 端口访问，用于访问前置机。
192.168.1.0/24	TCP	3306	允许	1	允许来自 FrontEnd 的 MySQL (3306) 端口访问

配置完成后如下图：



----结束

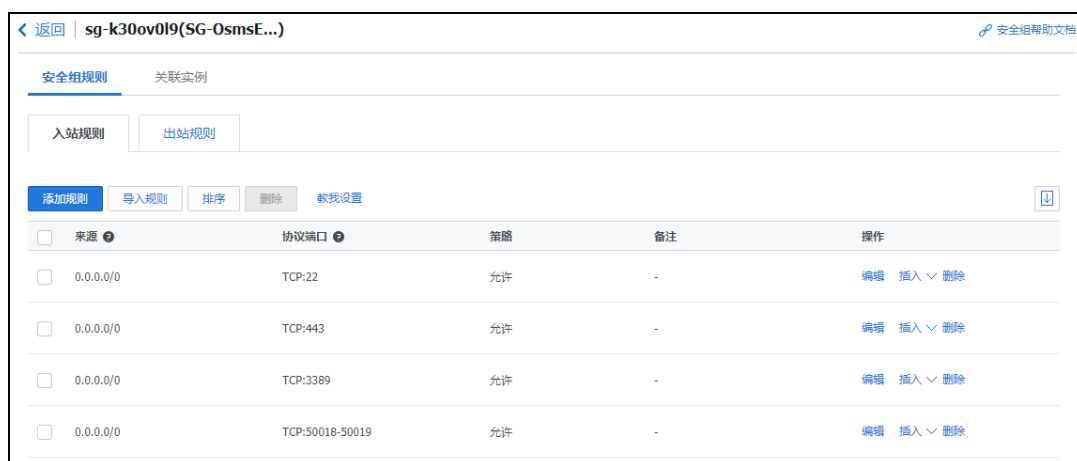
4.4.4 OsmsEnd 的安全组

创建一个名为 “SG-OsmsEnd” 的安全组，配置方式见 4.3.1 节。

入站规则要点为：

来源	协议	端口	访问	优先级	说明
Internet	TCP	22	允许	100	用于通过字符模式对设备进行管理
Internet	TCP	443	允许	101	用于访问堡垒机管理页面
Internet	TCP	3389	允许	102	用于通过 RDP 协议对设备进行管理
Internet	TCP	50018	允许	103	用于 RDP/VNC 老架构图形代理
Internet	TCP	50019	允许	104	用于图形日志回放和新架构实时查看

配置完成后如下图：



----结束

4.5 创建 Server 实例

分别在 FrontEnd 和 BackEnd 中各部署 1 个云主机，DB Server 选择不分配公网 IP，并分配各自的安全组 SG_FrontEnd 和 SG_BackEnd，使其不能被公网访问。

实例创建成功后，分别在 db-1 上安装了 My SQL，在 web-1 上安装了一个 web server，用于完成本示例的演示。

----结束

4.6 部署 vOSMS 实例

在 OsmsEnd 子网中创建 1 个 OSMS 实例 “osms”。

ID/主机名	监控	状态	可用区	主机类型	配置	主IP地址	主机计费模式
ins-et08cm1p vOSMS		运行中	北京三区	标准型S2	2核 4GB 1Mbps 系统盘：普通云硬盘 网络：TestVPC	140.143.193.211 (...) 192.168.4.11 (内)	按量计费 2018-06-25 10:22 创建


在腾讯云上，可以有三种方式创建 vOSMS 实例，分别加以介绍：

- 从云市场上创建新实例
- 从控制台上创建新实例
- 使用现有的空闲云主机

4.6.1 从云市场创建新实例

步骤 1 访问腾讯云首页，选择菜单 **云市场**，在搜索框中输入“绿盟堡垒机云服务（BYOL）”，即可看到绿盟科技的 vOSMS 产品，选择立即购买。

步骤 2 开始根据此镜像创建云主机，本例中云主机资源选择的是 S3.MEDIUM4（vCPU：2 核，内存：4G），存储：100G

 注意	<ol style="list-style-type: none"> 1. 由于本文只是出于演示和快速实践的目的，所以在生产环境中使用时，请根据已经选择绿盟堡垒机云服务规格，其对应的建议虚拟机资源需求来创建云主机。 2. vOSMS 需要一个公网 IP，可以采用在创建云主机过程中选择“分配公网 IP 地址”，也可稍后分配弹性 IP 的方式
--	--



步骤 3 在创建云主机的最后一步，会要求设置密码或者密钥对，从而能通过 SSH 安全登录实例。对于 vOSMS 实例来说，设置密码并不能对实例生效，同时也不支持将您的私有密钥导入，同时默认也不会开启 22 端口，您此处直接点击“立即购买”的按钮继续即可。

步骤 4 创建好的关键信息如下：

^ 地域和机型 编辑	
主机计费模式	包年包月
地域	北京
可用区	北京一区
所属网络	vpc-gayn3i14 TestVPC 192.168.0.0/16
所在子网	subnet-8aphhp6h OsmsEnd 192.168.3.0/24
机型	S3.MEDIUM4 (标准型S3, 2核4GB)

^ 镜像 编辑	
镜像	镜像市场
镜像信息	<div style="border: 1px solid #ccc; padding: 5px;"> <p>绿盟网站安全防护服务 (BYOL)</p> <p>镜像ID : img-a5jn8yyd 操作系统 : FreeBSD 10.0 64位 镜像大小 : 73GB 提供商 : 北京神州绿盟科技有限公司 集成软件 : Linux</p> </div>

4.6.2 从控制台创建新实例

步骤 1 访问腾讯云控制台，选择菜单 **云服务器**，在云主机部分，点击新建云主机

步骤 2 选择**镜像市场**，从镜像市场选择：**绿盟堡垒机云服务 (BYOL)**，点击使用

选择镜像 ×

<p>服务市场</p> <p>基础环境</p> <p>全能环境</p> <p>管理与监控</p> <p>安全高可用</p> <p>Docker容器</p> <p>业务管理</p> <p>操作系统</p>	<p>绿盟网站安全防护服务 (BYOL)</p> <p>操作系统 : FreeBSD 10.0 64位</p> <p>集成软件 : Linux</p> <p>集成软件 : 北京神州绿盟科技有限公司</p>	<div style="border: 2px solid orange; padding: 2px; display: inline-block; color: white; font-weight: bold;">免费使用</div> 同意用户协议
<p>绿盟堡垒机云服务 (BYOL)</p> <p>操作系统 : CentOS 5.0</p> <p>集成软件 : Linux</p> <p>集成软件 : 北京神州绿盟科技有限公司</p>	<div style="border: 2px solid orange; padding: 2px; display: inline-block; color: white; font-weight: bold;">免费使用</div> 同意用户协议	

绿盟

快速配置
自定义配置

1.选择地域与机型
2.选择镜像
3.选择存储和带宽
4.设置安全组和主机
5.确认配置信息

镜像

公共镜像
自定义镜像
共享镜像
镜像市场 ②

绿盟网站安全防护服务 (BYOL) V1.0.0 [重新选择](#)

上一步

下一步: 选择存储和带宽

步骤 3 云主机创建的后续步骤及要求等同于上一小章节

4.6.3 使用空闲云主机

使用现有空闲云主机可以有效利用已经购买的资源，一定程度上减少云主机的新花费



使用前请先确认准备使用的空闲云主机资源是否满足 vOSMS 的资源要求
如果虚拟资源不满足需要，则需要再额外增加虚拟资源，如系统盘大小等

步骤 1 访问腾讯云控制台，选择菜单 **云主机**

步骤 2 选择 **重装系统**，从服务市场选择：**绿盟堡垒机云服务（BYOL）**，点击 **确认更换**

重装系统 ×

您已选 1台云主机，[查看详情](#) ▾

No.	主机名	主机ID	系统盘大小	操作系统
1	vOSMS	ins-et08cmlp	73GB	FreeBSD 10.0 64位

注意：重装后，服务器系统盘内的所有数据将被清除，恢复到初始状态；服务器数据盘的数据不会丢失，但需要手动挂载才能使用，具体请参看 [操作指引](#)

镜像来源 当前镜像 公共镜像 自定义镜像 共享镜像 服务市场

镜像 基础环境 全能环境 管理与监控 安全高可用 Docker容器 业务管理 操作系统

绿盟堡垒机云服务（BYOL） ▾

免费开通DDos防护和云镜主机防护 [安全加固介绍](#)

免费开通云产品监控、分析和实时告警 [云监控介绍](#)

系统盘  100 GB 500GB

[系统盘扩容介绍](#)

步骤 3 云主机创建的后续步骤及要求等同于上一小章节

----结束

4.7 创建前置机实例

使用堡垒机数据库图形审计功能，需要在 BackEnd 子网创建一台 Windows Server2008 虚拟机作为前置机

配置方面，需要开启该 Windows Server 的远程桌面访问，并根据需要安装对应的客户端软件，如 MySQL 的客户端工具

5 导入许可证和快速配置

本章主要包含以下内容：

功能	描述
访问 vOSMS 的管理页面	配置 vOSMS 的管理页面访问方式。
导入许可证	介绍如何导入许可证。
配置字符审计	介绍如何在 vOSMS 上快速配置管理的虚拟机。
配置前置机数据库图形审计	介绍如何在 vOSMS 上快速配置前置机。

经过第四章环境部署后我们得到如下图所示环境拓扑，本章堡垒机配置均基于该环境拓扑。

5.1 对 vOSMS 进行管理

本例中 vOSMS 的管理端口是 443，本示例中通过公网访问的方式对 vOSMS 加以管理，在上一章中 vOSMS 管理子网允许通过互联网访问 443 端口。



注意

管理端口默认是 443，也可以在管理页面中加以修改为其他端口

以 vOSMS 为例：

步骤 1 获取 vOSMS 的公网 IP。

<input type="checkbox"/>	ID/主机名	监控	状态	可用区	主机类型	配置	主IP地址	主机计费模式
<input type="checkbox"/>	ins-et08cmlp vOSMS		运行中	北京三区	标准型S2	2核 4GB 1Mbps 系统盘：普通云硬盘 网络：TestVPC	140.143.193.211 (...) 192.168.4.11 (内)	按量计费 2018-06-25 10:22 创建

通过控制台创建的堡垒机具有一个弹性的公网 IP，如上图所示为：140.143.193.211

步骤 2 通过浏览器访问 <https://140.143.193.211>，可进入 vOSMS 的管理页。



----结束

5.2 导入许可证

在导入许可证之前，vOSMS 不能正常使用，所以必须导入合法的许可证。导入许可证的具体步骤如下所示：

- 步骤 1** 通过浏览器访问 [https:// 140.143.193.211](https://140.143.193.211)，可进入 vOSMS 的授权认证页面。
- 步骤 2** 本地 IP 地址填写堡垒机所在虚拟机内网 IP。
- 步骤 3** 单击【浏览】，弹出选择许可证文件窗口。
- 步骤 4** 选择许可证文件，单击【打开】按钮。
- 步骤 5** 单击【提交】按钮，上传许可证文件。
- 步骤 6** 等待云端授权完成。



----结束

5.3 配置字符审计

使用运维管理员（supervisor）完成所有配置后，用户可以使用支持 SSH 协议的第三方客户端工具通过堡垒机访问 SSH 协议的目标设备。



本例中为了验证过程，使用了 vOSMS 自带的运维管理员(supervisor)帐号，正式使用时，建议创建不同的用户来满足安全运维的要求。

对基于 SSH 协议的操作，系统可以完整记录用户在设备上的所有操作，并可实时监控对设备的命令操作。通过查看字符审计日志，可以方便审计管理员、运维管理员和设备管理员对正在进行或已结束的字符会话数据进行分析。

步骤 1 以运维管理员身份（supervisor）登录堡垒机，选择菜单设备管理>设备>设备，进入设备对象的配置。



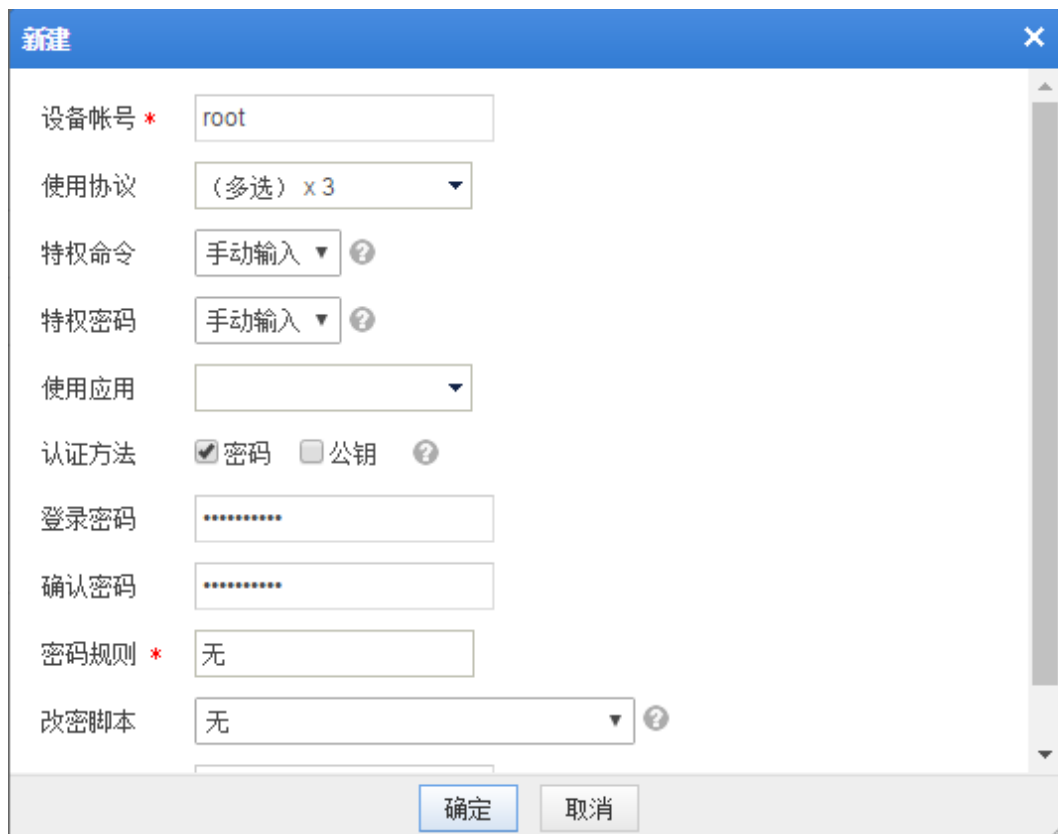
步骤 2 新建设备，在上图所示的设备对象列表的右上方，单击【新建】进入新建设备对象的页面

设备		设备组	孤儿设备	设备发现	前置机	应用平台
Name *	<input type="text" value="请输入设备名称"/>	部门	<input type="text"/>			
业务类型	<input type="text" value="详情"/>	Comment	<input type="text"/>			
资产级别	<input checked="" type="radio"/> 一般资产 <input type="radio"/> 重要资产 <input type="radio"/> 核心资产					
设备类型	UNIX/LINUX服务器					
设备IP *	<input type="text" value="0.0.0.0"/> <input type="button" value="ping"/>	设备协议	<input type="text" value="请选择设备协议"/>	<input type="button" value="端口检测"/>		
登录方式	<input checked="" type="radio"/> 全局配置 <input type="radio"/> 自定义 <input type="radio"/> 自动登录 <input type="radio"/> 手动登录	应用程序	<input type="text" value="请选择应用程序"/>			
特权配置 <<						
特权命令	<input type="text"/>	密码提示	<input type="text" value="assword:"/>			
特权密码	<input type="text"/>	确认密码	<input type="text"/>			
sudo密码提示	<input type="text" value="assword:"/>					
改密配置 <<						
改密脚本	<input type="text" value="None"/>	密码规则	<input type="text" value="None"/>			
高级配置 <<						
会话空闲超时(分) *	<input type="text" value="0"/>	设备编码	<input checked="" type="radio"/> UTF-8 <input type="radio"/> GBK			
登录提示	<input type="text" value="ogin:"/> <input type="checkbox"/> Enable	密码提示	<input type="text" value="assword:"/> <input type="checkbox"/> Enable			
阻断字符	<input type="text"/>	换行符	<input type="text"/>			
<input type="button" value="保存"/>		<input type="button" value="保存并添加帐号"/>		<input type="button" value="返回"/>		

步骤 3 填写设备名称，设备 IP，设备协议选择 SSH 等使用 22 端口协议后保存并添加账号

设备		设备组	孤儿设备	设备发现	前置机	应用平台
名称 *	<input type="text" value="web-1"/>	部门	<input type="text"/>			
业务类型	<input type="text" value="详情"/>	备注	<input type="text"/>			
资产级别	<input checked="" type="radio"/> 一般资产 <input type="radio"/> 重要资产 <input type="radio"/> 核心资产					
设备类型	UNIX/LINUX服务器					
设备IP *	<input type="text" value="192.168.1.53"/> <input type="button" value="ping"/>	设备协议	SSH,SFTP,SCP	<input type="button" value="端口检测"/>		
登录方式	<input checked="" type="radio"/> 全局配置 <input type="radio"/> 自定义 <input type="radio"/> 自动登录 <input type="radio"/> 手动登录	应用程序	<input type="text" value="请选择应用程序"/>			

步骤 4 创建登录设备的账号信息，我们在 4.4 节创建的 Server 实例时创建了账号“root”，在这里选择密码认证，并填写创建实例时填写的密码。



步骤 5 使用同样的方式添加 db-1 设备，配置完成后如下图所示：



编号	名称	部门	设备类型	协议/应用	设备IP	设备管理员	备注	关联策略	操作
1	【一般资产】db-1		UNIX.LINUX服务器	SSH 22,SFTP 22,SCP 22	192.168.2.183	supervisor(supervisor)		+	删除
2	【一般资产】web-1		UNIX.LINUX服务器	SSH 22,SFTP 22,SCP 22	192.168.1.53	supervisor(supervisor)		+	删除

步骤 6 打开终端，使用运维管理员账号（supervisor）通过 ssh 登录堡垒机。

```
# tan @ tanyawei-pc in ~ [13:32:25]
$ TERM=xterm ssh supervisor@119.23.226.67
Password: [ ]
```

步骤 7 输入“1”进入设备列表选择需要连接的设备。

```

-----
-- Welcome to Terminal Menu --
-----
[1] > Start New Selection.(UTF-8 character)
[2] > Start New Selection.(GBK character)

[q] < Quit.

Choice: 1
-----
-- Device List --
-----
[1] > 192.168.2.183 (db-1)
[2] > 192.168.1.53 (web-1)

[s] < Search
[b] < Back to select the type of encoding
[q] < Quit

Choice: [

```

步骤 8 输入“1”选择 web-1 作为示例，选择设备后继续选择登录协议及登录账号登录设备。

```

-----
-- Device Protocols --
-----
[1] > SSH:22

[b] < Back to select the device
[q] < Quit

Choice: 1
-----
-- Device Users --
-----
[1] > root

[b] < Back to select the device protocol
[q] < Quit

Choice: [

```

步骤 9 验证登录信息。

```

Prepare to login to the target device, Please wait a second.

Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-85-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Welcome to Alibaba Cloud Elastic Compute Service !

root@iZwz9f46qhpa7oqbb9pyprZ:~# [

```

步骤 10 以运维管理员身份（supervisor）登录堡垒机，选择菜单日志分析>字符审计，进入字符审计日志查询条件页面。

条件

访问时间: 2017-08-04 12:35:22 - 2017-08-04 13:35:22

会话类型: 未选择

报表类型: word excel

更多 <<

用户: 登录IP:

设备名称: 设备IP:

会话ID: 运维备注:

协议: 全部

命令导出: 是 否

命令/结果关键字: 搜索命令执行结果

危险级别: 全部 低 中 高

动作: 全部 阻断 允许

资产级别: 核心资产 重要资产 一般资产

查询

步骤 11 设定好指定的查询条件后，单击页面左下方的【查询】，进入字符审计日志列表页面。

会话ID	登录时间	断开时间	用户	设备	设备编号	协议	危险等级	运维备注	操作
2	2017-08-04 13:35:18		supervisor (119.97.214.138)	web-1(192.168.1.53)	root	SSH	中		
1	2017-08-04 13:34:22	2017-08-04 13:35:04	supervisor (119.97.214.138)	db-1(192.168.2.183)	root	SSH	中		

----结束

5.4 配置前置机数据库图形审计

用户可通过配置前置机进行数据库服务器的图形审计，运维人员可通过堡垒机访问数据库服务器，对服务器进行访问（用户使用手动方式登录），同时可对运维人员在服务器的所有操作进行图形化审计，针对数据库图形审计日志，用户可以进行的相关操作有回放操作、查看键盘日志、下载图形审计日志。

步骤 1 以审计管理员（auditor）登录，开启数据库审计功能。选择菜单**系统管理>审计参数配置**，进入审计参数配置页面，开启数据库审计，参数配置如下图所示。单击【确定】完成配置。

审计日志参数 ^

会话日志记录 启用 禁用 ?

会话合规审计 字符日志 图形日志 文件日志 网页URL日志 网页图形日志 数据库图形日志

窗口标题日志记录 启用 禁用 ?


[高级选项>>](#)

命令查看 启用 禁用

字符日志回放 启用 禁用

字符日志命令结果查看 启用 禁用

图形键盘日志 启用 禁用

步骤 2 以运维管理员身份（supervisor）登录堡垒机，下载堡垒机前置机代理程序，并在前置机中安装。选择菜单**运维管理>工具下载>前置机代理程序**，进入前置机代理程序页面。单击前置机代理程序对应的，下载程序并将其安装在前置机中。

步骤 3 新建前置机对象。选择菜单**设备管理>设备>前置机**，进入前置机对象列表页面。单击前置机列表右上角的【新建】，新建一个数据库前置机。

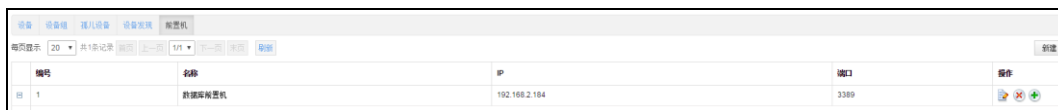
新建 ×


名称 *	<input type="text" value="数据库前置机"/>
IP *	<input type="text" value="192.168.2.184"/>
协议 *	<input type="text" value="RDP"/>
端口 *	<input type="text" value="3389"/>
前置机代理别名	<input type="text" value="dbLogin32"/>
前置机代理路径	<input type="text" value="C:\SAS-H\bin\dbLogin32.exe"/>
登录帐号	<input type="text"/>
登录密码	<input type="password"/>
确认密码	<input type="password"/>
部门	<input type="text"/>
备注	<input style="height: 30px;" type="text"/>

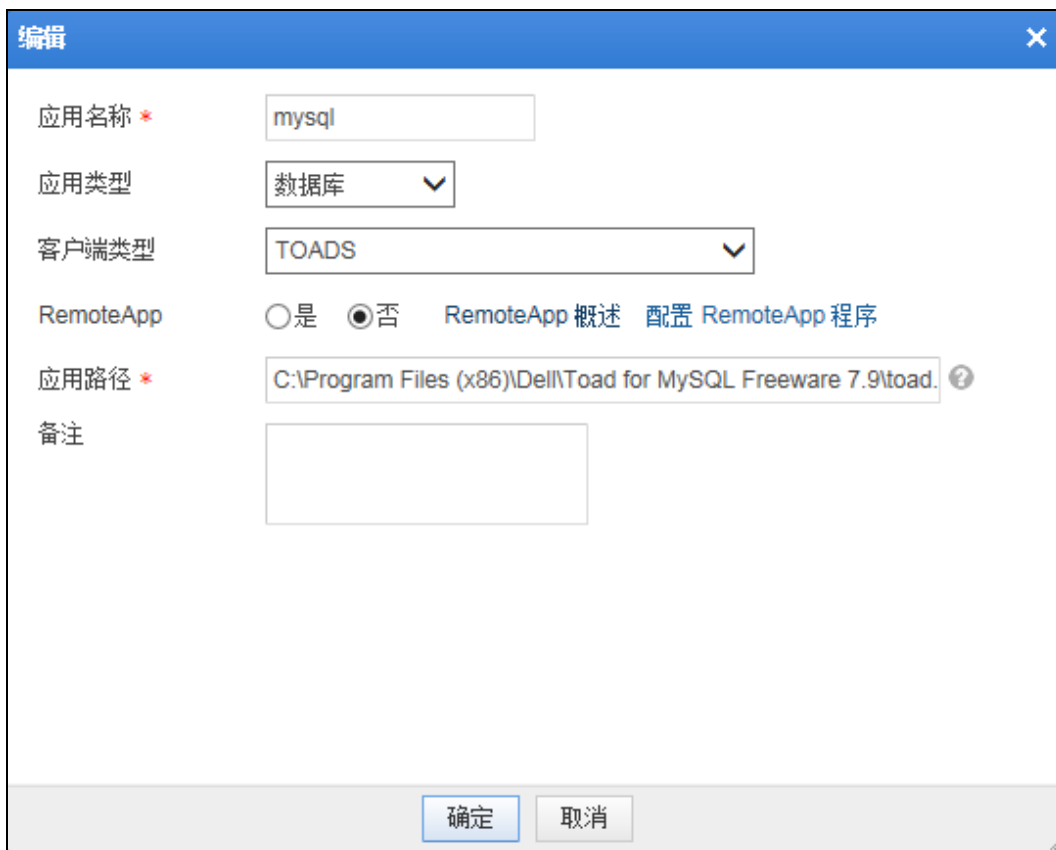


配置前置机对象时，协议必须选择 RDP，端口根据前置机提供的 RDP 协议的端口进行配置，默认为 3389。

步骤 4 单击【确定】完成配置，回到前置机对象列表页面



步骤 5 在数据库前置机对应的操作栏中单击图标,为数据库前置机添加一条应用程序 mysql, 如图所示。



说明

应用路径为输入 mysql 管理客户端 TOADS 应用程序所在的路径，也就是数据库管理客户端的安装路径，请确保输入的路径正确，否则前置机配置无法生效。

步骤 6 新建设备对象。选择菜单**设备管理>设备**，进入设备列表页面。单击设备列表右上角的【新建】，新建一个“MySQL 服务器”设备，各项配置如图所示。单击【保存】完成配置。

步骤 7 选择菜单**运维管理>设备访问**，选择“数据库服务器”，然后点击设备名称，如图所示：

步骤 8 输入帐号和密码，并选择应用、服务器信息，然后点击【远程桌面】即可对设备进行运维。

步骤 9 以设备管理员（supervisor）登录堡垒机，选择菜单**日志分析>数据库审计>数据库图形**，可以查看产生的数据库图形审计日志。

会话ID	登录时间	断开时间	用户	设备	设备帐号	协议	风险等级	运维备注	操作
14	2017-08-04 15:48:41	2017-08-04 15:48:41	supervisor (119.97.214.138)	MySQL服务器(192.168.2.183)		RDP	🔴		🔍 🔄 🗑️
10	2017-08-04 15:45:31	2017-08-04 15:45:31	supervisor (119.97.214.138)	MySQL服务器(192.168.2.183)	supervisor	RDP	🔴		🔍 🔄 🗑️
9	2017-08-04 15:44:57	2017-08-04 15:44:57	supervisor (119.97.214.138)	MySQL服务器(192.168.2.183)	supervisor	RDP	🔴		🔍 🔄 🗑️
8	2017-08-04 15:44:44	2017-08-04 15:44:44	supervisor (119.97.214.138)	MySQL服务器(192.168.2.183)		RDP	🔴		🔍 🔄 🗑️
7	2017-08-04 15:44:26	2017-08-04 15:44:26	supervisor (119.97.214.138)	MySQL服务器(192.168.2.183)		RDP	🔴		🔍 🔄 🗑️

----结束

5.5 配置短信认证

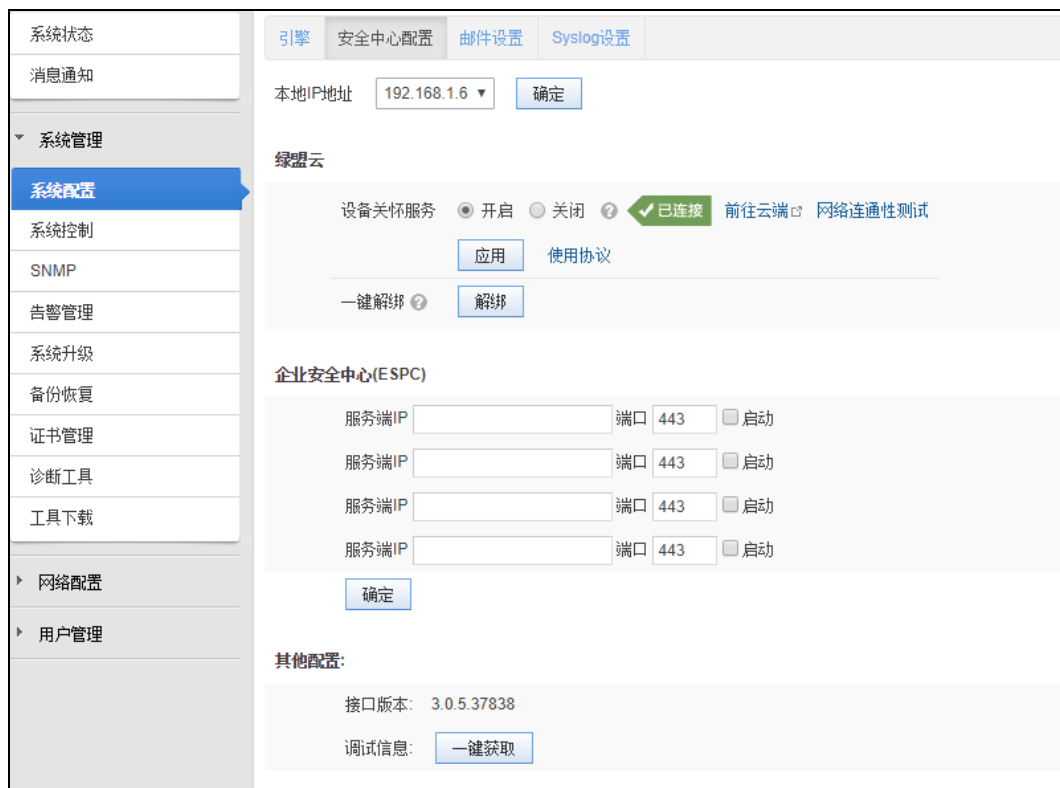
vOSMS 支持多种方式的双因子认证方式，本例中介绍本地认证+短信认证的方式。



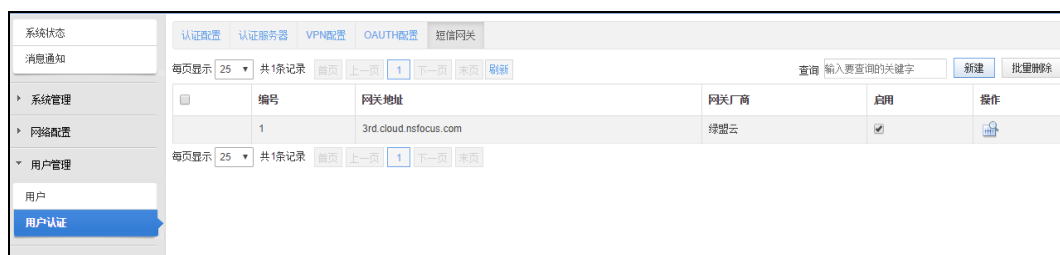
- 只有堡垒机管理员可以配置短信网关，同时可以支持多种短信网关。
- 只有审计员、普通用户和设备管理员角色支持短信认证。
- 堡垒机内置的帐号都不支持短信认证，新建帐号都支持。

以堡垒机管理员（admin）登录，进行如下配置：

步骤 1 进入系统配置，系统管理>系统配置>安全中心配置，配置本地 IP 地址，同时开启 设备关怀服务，点击【应用】完成配置。



步骤 2 选择菜单用户管理>用户认证>短信网关，进入短信网关页面。选择“绿盟云”提供的短信网关，单击【启用】。



步骤 3 修改认证配置。选择菜单用户管理>用户认证>认证配置，进入认证配置页面。设置认证方式为本地认证+短信认证。



步骤 4 新建普通用户。选择菜单**用户管理>用户**，单击用户列表右上角的【新建】，新建普通用户，注意需要填写正确的手机号，认证选项选择 **全局配置**，单击【保存】完成配置。



编号	用户名	真实姓名	部门	角色	允许登录IP	认证模式	创建者	数字证书	启用	操作
1	admin	admin		系统机管理员	*	自定义 本地认证			启用	
3	supervisor	supervisor		运维管理员	*	自定义 本地认证			启用	
5	zhangsan	张三		普通用户	*	自定义 本地认证 + 短信认证	admin		<input checked="" type="checkbox"/>	

步骤 5 普通用户登陆堡垒机，此时可以按照界面提示收取短信进行双因子认证登陆。

----结束

6 其他配置说明

本章主要包含以下内容：

功能	描述
vOSMS 的默认账号密码	修改默认账号密码。
端口说明	介绍需要开放的端口。

6.1 初始用户

请您将 vOSMS 启动后，尽快将初始账号密码进行修改。

	用户名	密码
堡垒机管理员	admin	admin
审计管理员	auditor	auditor
运维管理员	supervisor	supervisor

6.2 端口说明

vOSMS 中，如果需要配置使用一些额外功能，需要将相应端口在安全组中放开。vOSMS 中主要服务端口说明如下：

端口	使用描述
22	以 SSH 协议访问堡垒机时，必须开启该端口。
139/445	启用 RDP 会话文件共享后，必须开启 139 和 445 端口来传送文件。
443	以 HTTPS 方式访问堡垒机 Web 页面时，必须开启该端口。

端口	使用描述
3389	MSTSC 第三方客户端连接堡垒机访问 rdp、X11 和 vnc 协议的目标设备时，必须开启该端口。
5900	VNC 第三方客户端连接堡垒机访问 VNC 协议的目标设备时，必须开启该端口。
50001	前置机交互程序（api_device_com.py）。
50018	RDP/VNC 老架构图形代理（NSProxy.jar）。
50019	图形日志回放和新架构实时查看（record_server.py）。

----结束

6.3 更多配置方式

更详细、全面的配置可参见《绿盟运维安全管理系统配置手册》、《绿盟运维安全管理系统用户手册》。

----结束