信域 Lite 产品阿里云部署使用指南

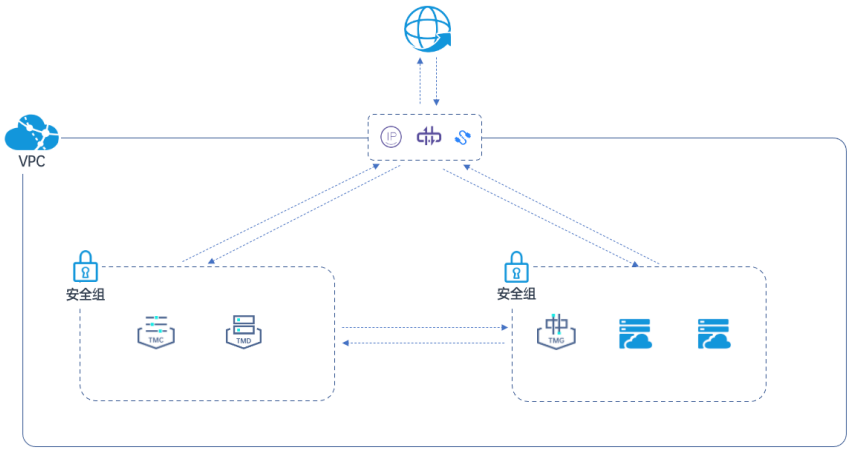
■ **文档编号**	请输入文档编号
■ **版本编号**	V1.0
■ **密级**	普通
■ **日期**	2022 年 6 月 18 日

信域安全云网的各个组件都可以部署在公有云环境中，支持在多云、混合云环境中部署，将企业的碎片化网络重新整合在一张安全的虚拟网络。

本文以在阿里云上安装部署信域组件为例，描述如何在公有云环境中部署信域安全云网。

信域组件部署拓扑

在云环境中部署信域安全云网的常见方式如下图所示：



- 如果企业的业务资源部署在公有云中，您希望将公有云里的业务资源发布到信域安全云网，方便终端用户在任意位置访问。您只需要在业务资源所在的安全组内再申请一台虚拟机，将 TMG 镜像导入到虚拟机中安装即可，申请的虚拟机无需额外的弹性公网 IP 和互联网带宽，直接复用 VPC 的公弹性公网 IP 和带宽即可，如图中右侧的安全组所示。
- 如果您希望将 TMC、TMD 等信域组件也部署在公有云里，建议您在 VPC 中单独建立一个安全组，将 TMC 和 TMD 部署在此安全组中。同样，TMC 和 TMD 也无需额外的弹性公网 IP 和互联网带宽，直接复用 VPC 的公弹性公网 IP 和带宽即可，如图中右侧的安全组所示。
- 您需要为部署不同信域组件的虚拟机开通相应的网络访问权限，关于网络权限的设置请参考：绎云科技官网-文档中心-物理网络访问权限要求。

在阿里云部署信域组件

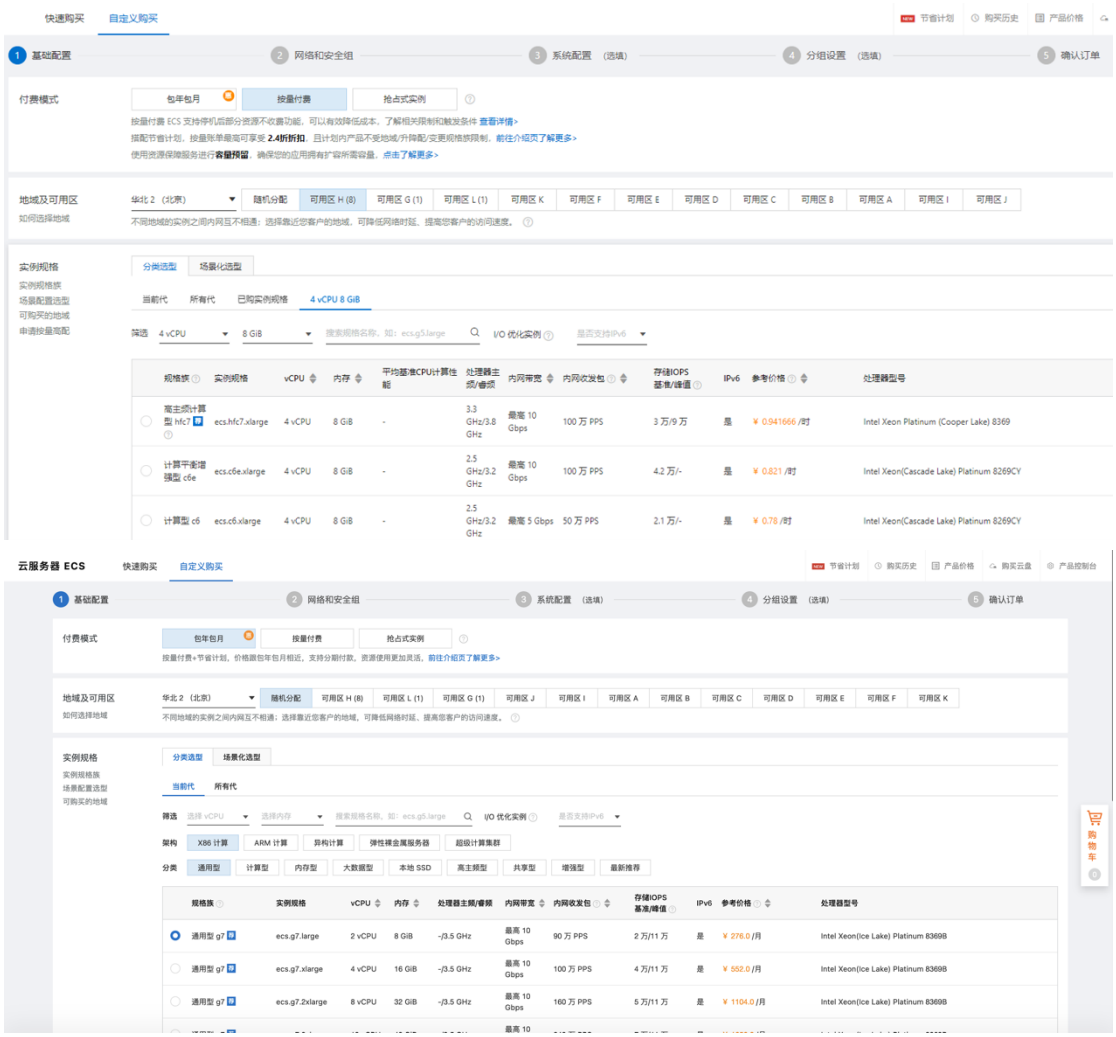
选购信域组件

在阿里云云市场的安全市场中搜索“信域”，您可以搜到信域 Lite 的 TMC、TMG、TMD 三个组件，如下图所示：

点击查看详情打开产品详情和购买页，如下图所示：

基础配置

点击“立即购买”即可进入自定义购买页面，在页面中选择购买实例的基础配置，如下图所示：



付费模式，地域以及可用区，可根据您的规划自行选择。实例规格需要选择 x86 架构，您可根据不同的需求选择相应的分类，推荐使用 “通用型” 和 “计算型” 。

如想了解不同类型的云主机特点，可查阅阿里云相关说明文档。

不同的虚拟机配置可以承载的网络规模和访问流量会有不同，具体的配置建议请参考：服务器配置建议。这里为了示范，选择最小配置为：4vCPU、8GiB 内存、100GiB 硬盘。

在镜像选择区，确认当前选择的镜像为刚才在云市场上购买的信域组件镜像，如下图所示：

如果您不是从云市场直接点击购买镜像进入的自定义购买页面，您需要在镜像选择配置区，选择“镜像市场”，点击“从镜像市场获取更多选择（含操作系统）”，如下图所示：

点击后，在镜像搜索页面的搜索条件输入框输入“信域安全云网”，你可以搜索到信域相关组件，点击“使用”可将对应的信域组件镜像作为虚拟机的安装镜像，如下图所示：

网络与安全组配置

点击下一步，进入“网络与安全组配置”页面，如下图所示：

选择信域组件计划部署的位置，包括：私有网络（VPC）、虚拟交换机。

注意：所选择的 VPC 和虚拟交换机需要具备公网 NAT 网关，以便信域组件可以通过 SNAT 方式与互联网通信，同时可以通 DNAT 方式配置 TMG 互联网映射 IP 地址和端口，以及让管理员可以远程登录信域组件的 WEB 控制台或 CLI 控制台管理配置信域组件。

如 VPC 网络已与本地管理员所在网络打通，则可以忽略 DNAT 方式远程访问信域组件的 WEB 控制台与 CLI 控制台。如果您的云上资源没有对 VPC 网络进行规划，也可以使用分配公网 IPv4 地址方式进行远程云主机的管理与使用（出于安全性考虑，不建议这种方式）。本例主要以 VPC 方式进行配置讲解。

点击选择安全组，为创建的虚拟机配置网络访问策略，如下图所示：

注意：我们建议安全组的组内联通策略，使用“组内互通”，如果您的安全组使用的是“组内隔离”则请参考物理网络访问权限要求。

关于阿里云安全组的使用说明，请参考阿里云官方文档。

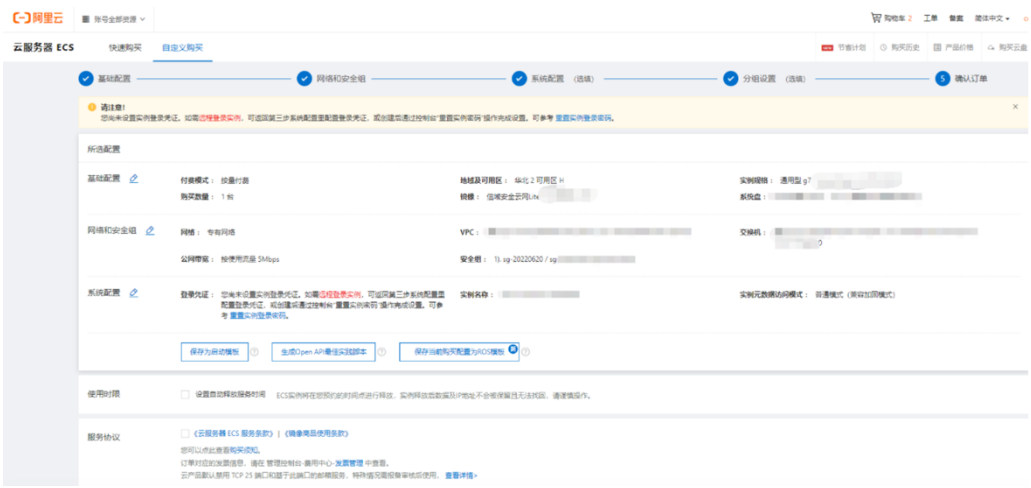
系统配置

点击“下一步：系统配置”完成虚拟机系统配置，如下图所示：

在“登录凭证”配置项，选择“创建后设置”。

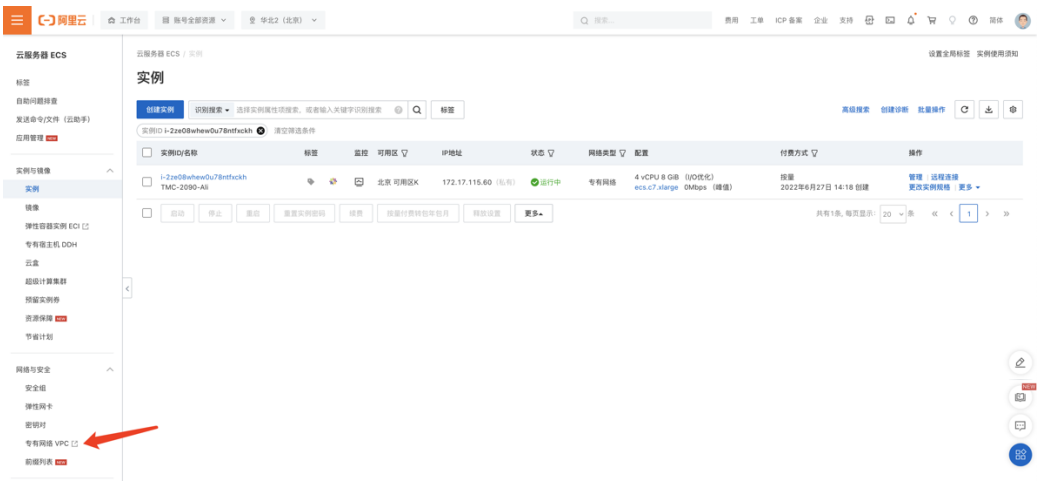
确认订单

点击“下一步：确认订单”，打开配置确认页，检查配置无误后点击“确认下单”完成配置过程，如下图所示：



VPC 网络配置

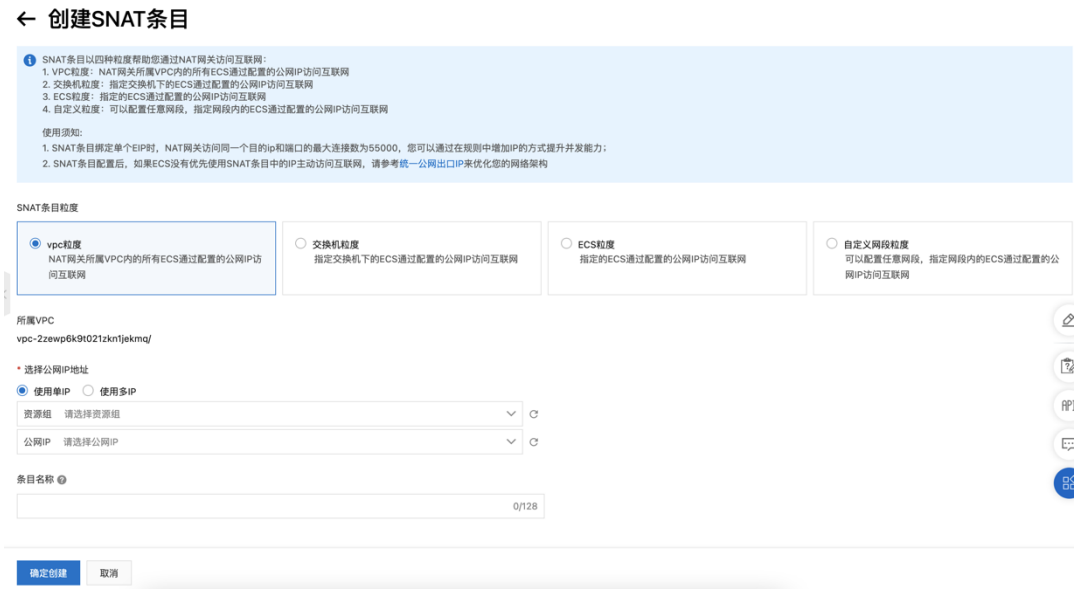
在云服务器 ECS 控制台，进入 VPC 管理页面，如下图所示：



选择【NAT 网关】->【公网 NAT 网关】，进入公网 NAT 网关配置页面。（如所使用的 VPC 中没有配置公网 NAT 网关，则需要创建，具体操作过程请参考阿里云官方文档。）

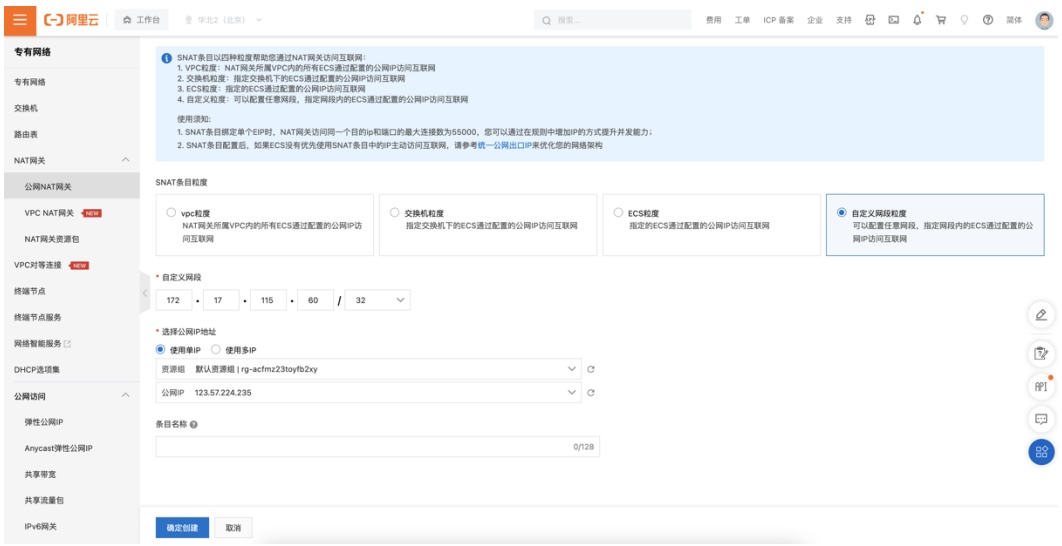
首先设置 SNAT，使组件可与互联网进行通信。

配置 SNAT 如下图所示：



阿里云提供了四种 SNAT 粒度，这里使用自定义网段粒度来做演示：

在自定义网段中填写刚刚创建的组件内网 IP，选择使用的公网 IP（推荐使用单 IP），配置完成后如下图所示：

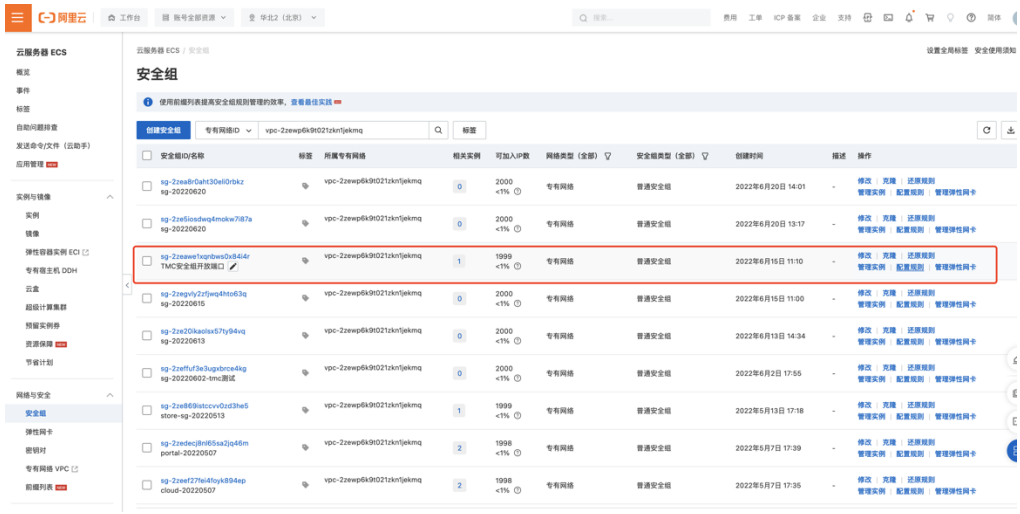


点击确认创建，完成 SNAT 配置。

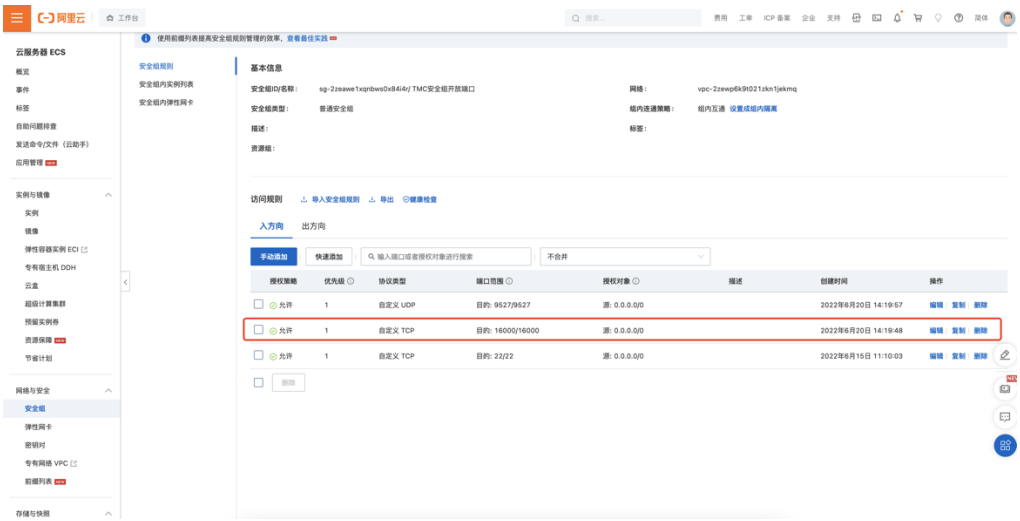
配置 DNAT，设置策略允许通过公网访问 TMC web 管理页面，如下图所示：

点击确认创建，完成 DNAT 配置。

注意：由于阿里云的安全组是基于 ECS 创建的，如果您想对 TMC WEB 管理页面做访问源 IP 的 ACL 访问控制，需要在创建组件时使用的安全组内进行修改，具体配置如下图所示：



选择配置规则，进入规则配置页面：



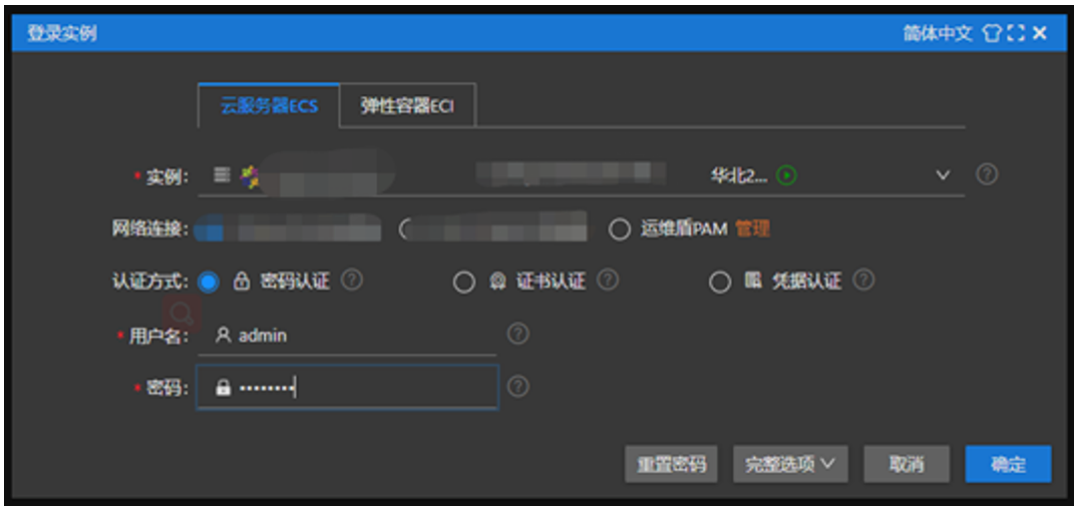
编辑入方向 16000 端口的规则，使其只开放管理员所在区域的出口 IP 地址权限。

以上完成了 TMC 组件的安装以及相关环境的配置，其他组件的操作与其类似，相关网络权限设置请参考绎云官网-文档中心-物理网络访问权限要求。

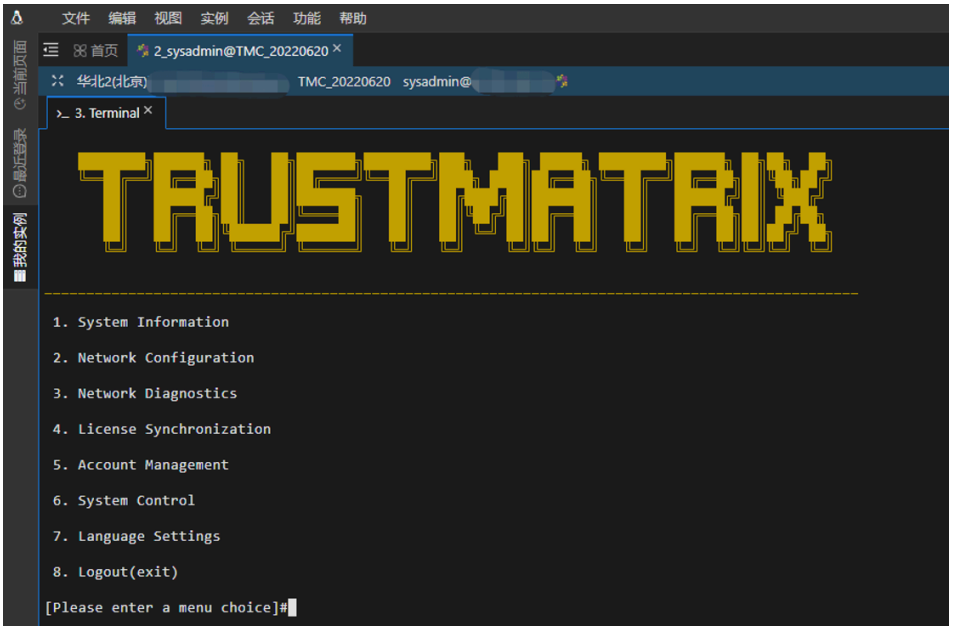
登录信域组件控制台

创建实例需要一点时间，创建完实例后，您可以在实例列表中查看到刚才创建的 TMC 实例，如下图所示：

在实例列表的操作列，点击“远程连接”可使用 Workbeach 连接 TMC 虚拟机控制台，登录配置里需要填入用户名：admin，密码：b4a5928c。



登录成功后您可以看到如下图所示的 TMC 控制台界面：



进入信域组件控制台界面后，您还需要使用您的信域企业帐号，通过同步授权证书激活信域组件。

信域其他组件在阿里云上的部署方式与 TMC 的部署方式大致相同，需要注意的是不同的组件对硬件配置和网络访问权限的要求会有不同，具体说明请参考：服务器配置建议、网络访问权限要求，本文不再一一赘述。