

智能边缘一体机专题

产品手册

产品手册

智能边缘一体机用户手册

整体介绍

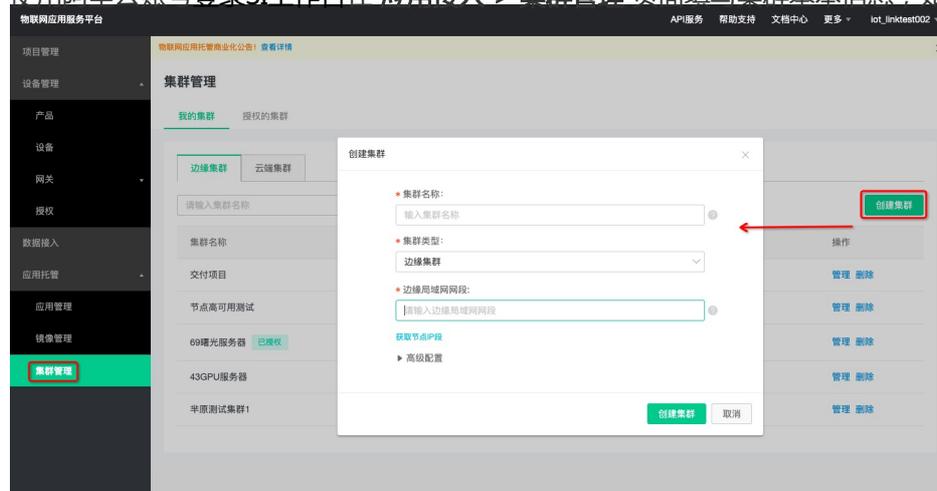
智能边缘一体机是一种新的边缘应用交付方式，它以开箱即用的方式，为运行于边缘现场的应用提供完整的应用生命周期管理、安全运行支撑、容灾容错保障、远程运维监控与报警等能力，本章将为您介绍整体的使用流程，其中包括：集群管理、应用管理、日常运维等。

1. 集群管理

集群可对多个主机设备进行管理，并且以集群为单位调度主机，同时部署应用时可指定部署集群。

1.1 创建集群

使用阿里云账号登录SIT工作台在 **应用接入 > 集群管理** 页面填写集群基本信息，如下图所示：



参数名称	参数说明
边缘集群	支持脱离公网，实现集群与应用边对边通讯。

智能边缘一体机集群	支持脱离公网，实现集群与应用边对边通讯，同时提供智能边缘一体机集群的集群组件。
存储地址	NFS服务器地址。
存储路径	NFS Mount路径。
服务地址段	边缘可用来分配的边缘服务网段。

建议使用与当前边缘局域网段不同的子网，否则有发生IP冲突的可能性导致服务异常。例如当前主机所在网络为192.168.1.0/24；可在路由器中再添加另一个子网192.168.2.0/24专门用来分配服务VIP。

接下来需要将边缘主机纳管。边缘主机分成两种，分为**添加智能边缘一体机节点**与**添加通用节点功能**，其中“智能边缘一体机节点”为阿里云IoT提供的硬件产品，但是在测试阶段，允许使用用户自己的主机进行调试，这种节点为“通用节点”。；

1.2创建EdgeBox节点

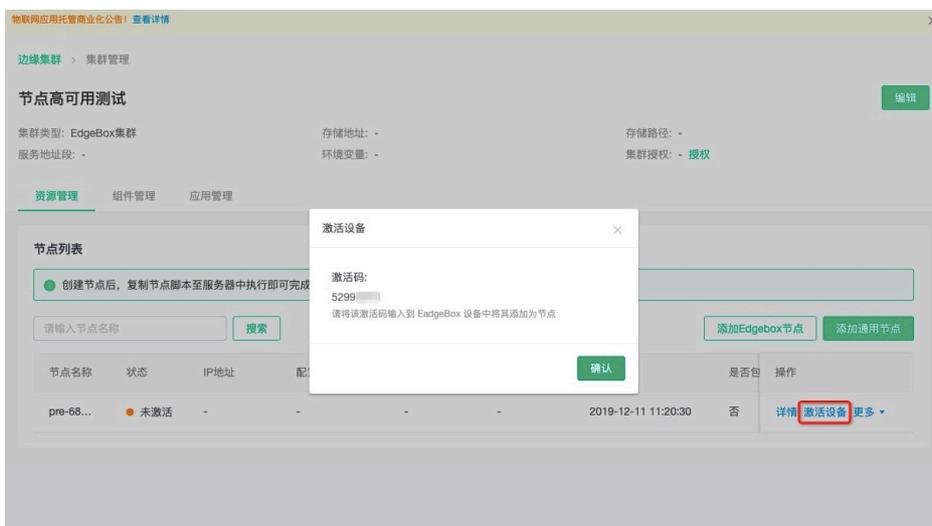
1.2.1添加节点

在 **管理 > 资源管理 > 添加智能边缘一体机节点** 页面填写节点基本信息，如下图所示：



参数名称	参数说明
节点名称	与集群名称不同，节点名称会被使用在K8S中，所以对命名有一定要求：只支持数字、小写英文、短划线，不能以短划线开头和结尾，长度限制4-30。
节点IP段	节点IP段为当前主机所在网段，需要用户提供以分配对应的Flannel Overlay服务网段。

选择创建的智能边缘一体机节点，单击**激活设备**，可获取主机激活码，如下图所示：



1.2.2 初始化系统

插入电源，主机开机后，将进入欢迎页面，您需要使用默认的用户名与密码登录系统（用户：owner；密码：change password），登录成功后会提示您是否需要修改密码。输入 Y：是，n：否，如下图所示：

```
*****
* Welcome to Edgebox Initial Setup *
*****
This Setup will guild you completing the Edgebox initialization process.
Do you want to change your password? [Y/n]:
█
```

设置成功后，将提示是否需要手动配置动态IP。输入 Y：是，n：否，如下图所示：

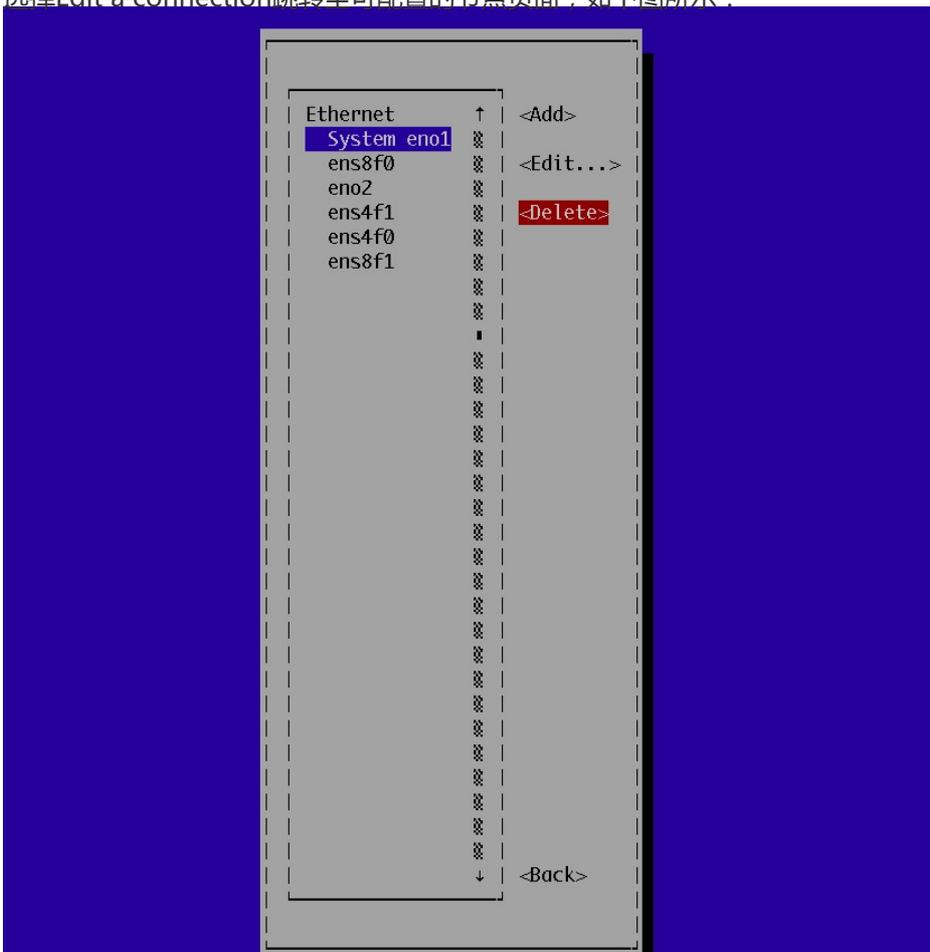
```
*****
* Welcome to Edgebox Initial Setup *
*****
This Setup will guild you completing the Edgebox initialization process.
Do you want to change your password? [Y/n]:
n
Merging home partition to root...
[sudo] password for owner:
Home partition is merged to root
Config network, do you want to use manual mode? [Y/n]:
y█
```

若选择Y后，将跳转至CentOs默认动态IP配置页面，如下图所示：

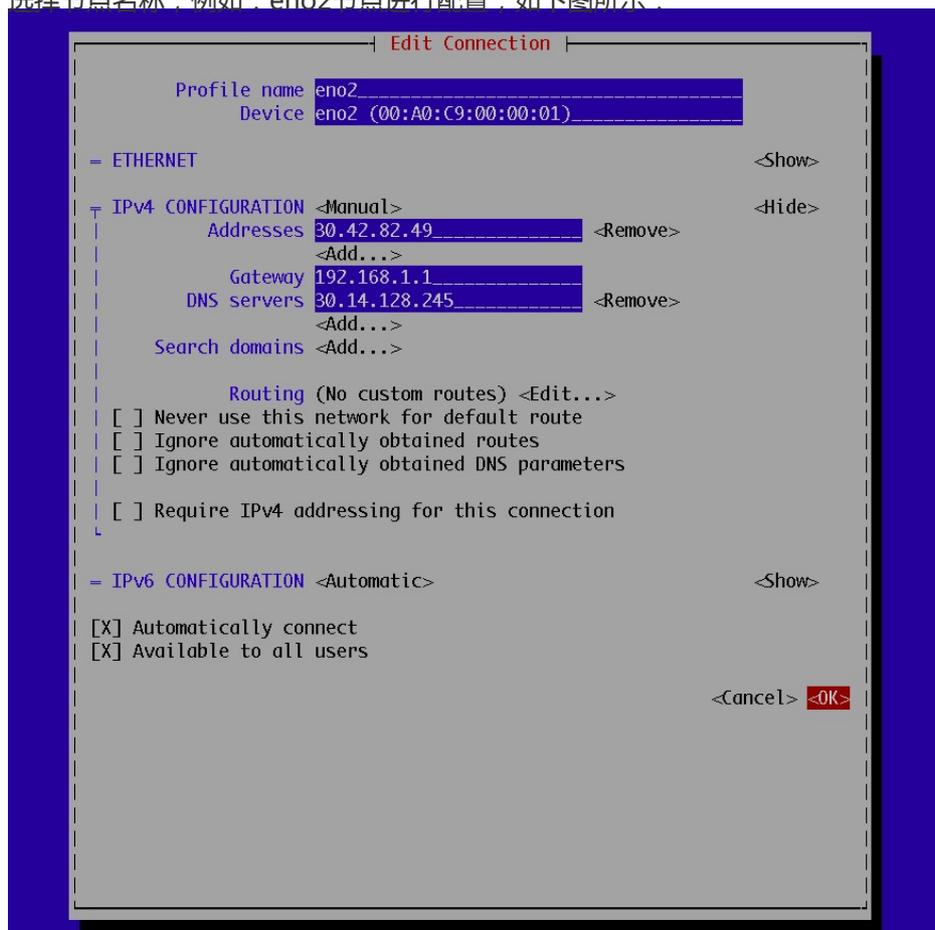


- Edit a connection : 创建一个新的连接。
- Activate a connection : 激活已配置的连接。
- Set system hostname ; 设置系统的主机名称。

选择Edit a connection跳转至可配置的节点页面，如下图所示：



选择节点名称，例如：eno2节点进行配置，如下图所示：

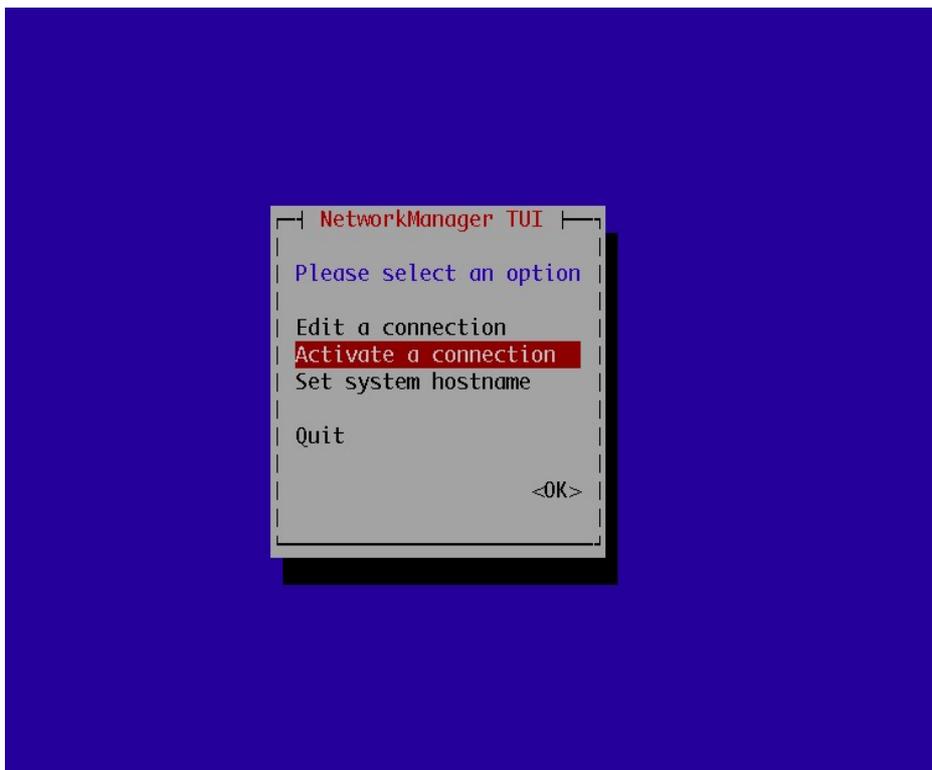


- Addresses：服务IP地址。
- Gateway：网关路由。
- DNS Servers：DNS区域解析。
- Automatically connect：自动连接。
- Available to all users：适用于所有用户。

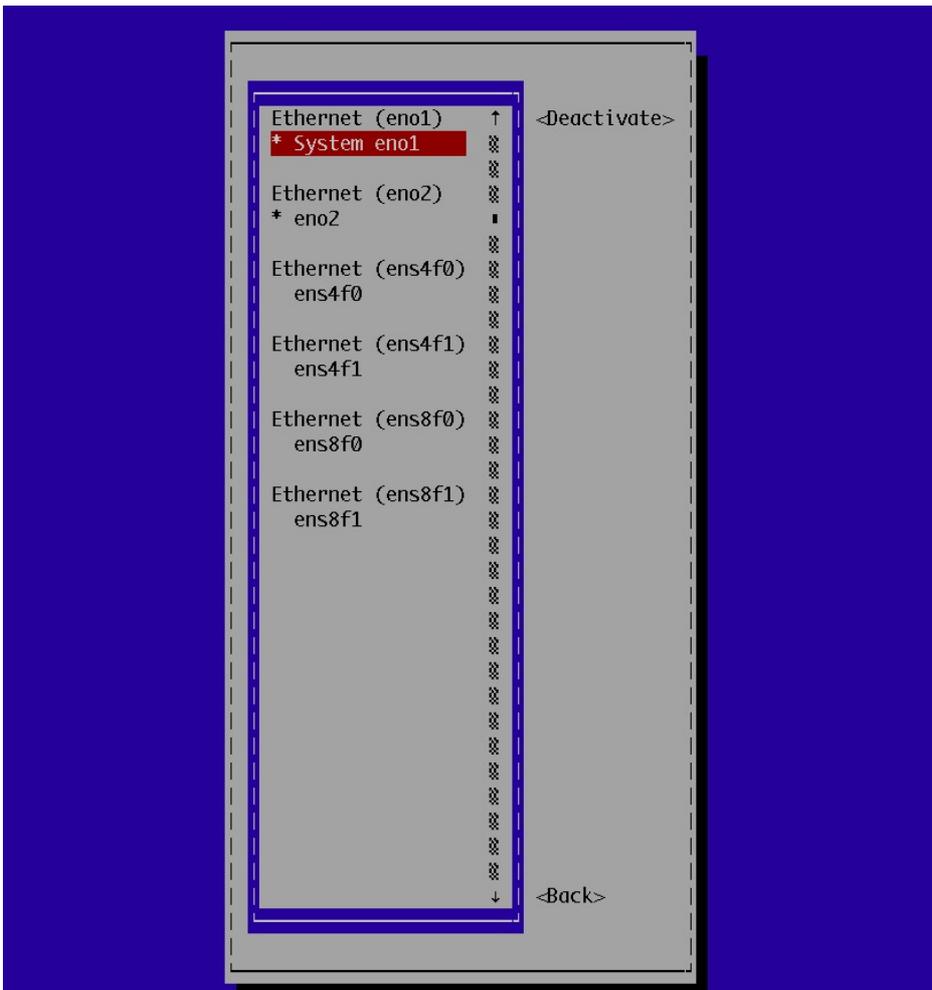
注意：

可将光标标记至名称前，敲击空格进行选定，建议将Automatically connect与Available to all users选项进行勾选，“X”为选中态。

配置完成后，将自动跳转至配置首页，选择Activate a connection，进行已配置服务IP激活，如下图所示：



"*" 标记为服务IP已经配置成功，可直接进行连接，如下图所示：



若选择n自动配置动态IP，将跳转至节点IP展示页面， eno1为动态获取的节点IP，eno2为上述手动配置的节点

```

Home partition is merged to root
Config network, do you want to use manual mode? [Y/n]:
n
[sudo] password for owner:
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 30.42.82.67 netmask 255.255.255.128 broadcast 30.42.82.127
    inet6 fe80::2a0:c9ff:fe00:0 prefixlen 64 scopeid 0x20<link>
    ether 00:a0:c9:00:00:00 txqueuelen 1000 (Ethernet)
    RX packets 124034 bytes 26442825 (25.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1060 bytes 191367 (186.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device memory 0x9d120000-9d13ffff

eno2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 30.42.82.49 netmask 255.255.255.255 broadcast 30.42.82.49
    inet6 fe80::502a:2b52:3971:39ee prefixlen 64 scopeid 0x20<link>
    ether 00:a0:c9:00:00:01 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device memory 0x9d100000-9d11ffff

ens4f0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 70:57:bf:f9:a1:24 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens4f1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 70:57:bf:f9:a1:26 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens8f0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 3c:fd:fe:d2:3d:bc txqueuelen 1000 (Ethernet)

```

IP，如下图所示：

动态IP配置完成后，将提示您是否需要设置设备名称与设备激活码，输入名称后选择回车即可生效，如下图所示：

```

Is this network configuration OK? [Y/n]:
y
Setup user account...
Please input name for this device:
device01
Please input user bind code:

```

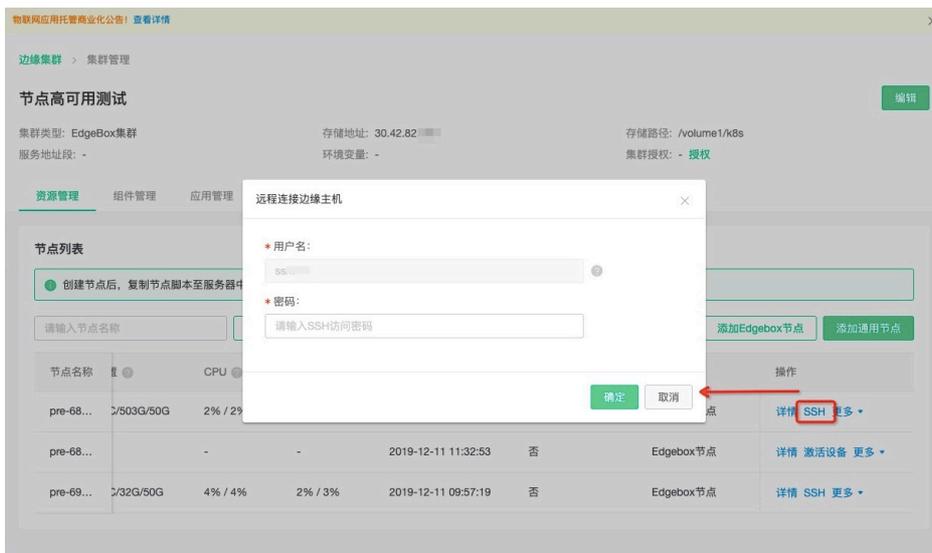
将通过激活设备获取到的激活码输入到主机中，如下图所示：

```

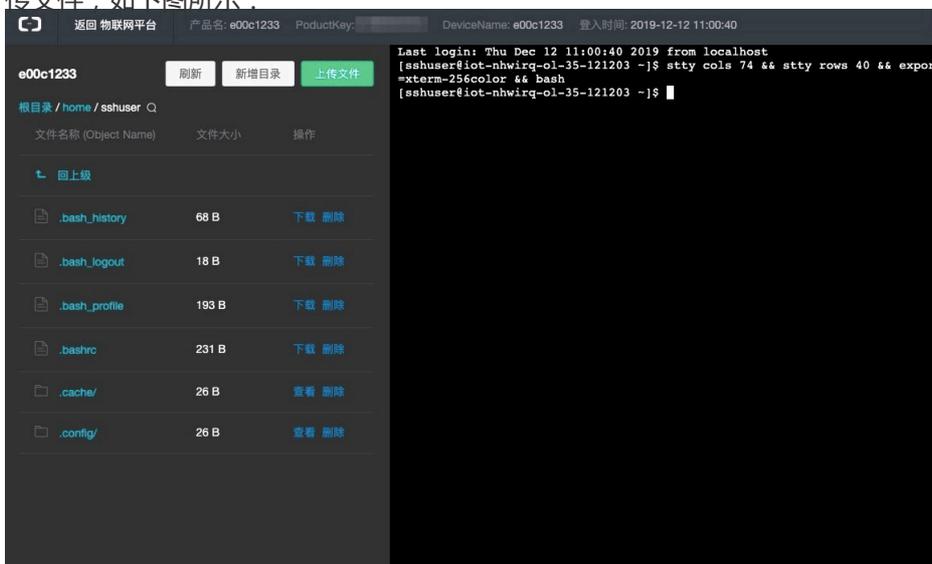
Is this network configuration OK? [Y/n]:
y
Setup user account...
Please input name for this device:
device01
Please input user bind code:
52995ded

```

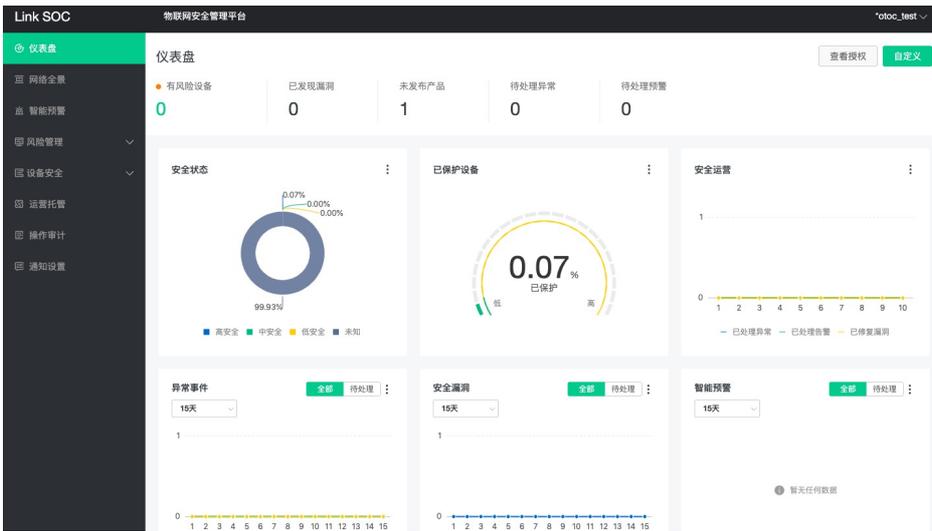
激活码输入后，将进行安全系统校验，DPS的相关认证，设备激活的输出日志。当出现successful为激活成功认证，如下图所示：



使用SSH远程登录成功后，跳转至主机控制台，对主机进行运维等操作，如需将文件传输至主机中，可单击上传文件，如下图所示：



选择运行中的智能边缘一体机节点，单击**更多**>**安全**，可跳转至安全管理平台，对已激活的主机进行管理，如下图所示：



1.3 添加通用节点

在 **管理 > 资源管理 > 添加通用节点** 页面填写节点基本信息，如下图所示：



参数名称	参数说明
节点名称	与集群名称不同，节点名称会被使用在K8S中，所以对命名有一定要求：只支持数字、小写英文、短划线，不能以短划线开头和结尾，长度限制4-30。
节点IP段	节点IP段为当前主机所在网段，需要用户提供以分配对应的Flannel Overlay服务网段。

节点创建完成后单击 **启动脚本 > 复制脚本** 到主机命令行执行，加入完成，节点状态将变成运行中，如下图所示：



1.4 组件管理（按需）

在 **组件管理** 页面，按照实际需要安装智能边缘一体机集群提供的集群组件，其中Link Visual集群组件需要先进行申请，由小二后台进行审核与配置，如下图所示：



注：

Link Visual平台对接文档：https://help.aliyun.com/document_detail/145374.html

Link IoT Edge平台对接文档：https://help.aliyun.com/document_detail/145370.html

2.应用管理

单击**集群管理**>**应用管理** 可查看部署在此集群的所有部署的应用列表与提供的集群组件信息，同时可以对已部署的应用进行测试，如下图所示：



3.运维管理

3.1应用运维

应用部署与升级中出现异常或需要对应用进行日常运维，您可以单击**实例管理**>**管理**在此页面进行操作，应用运维功能包括：日志、终端、扩容、升级等，如下图所示：

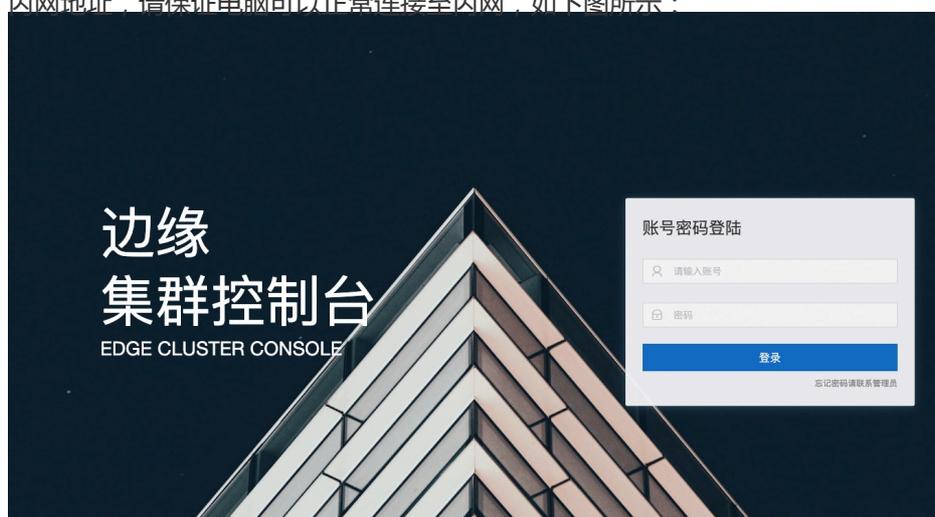


3.2控制台管理

单击**组件管理**>**访问入口**复制IP+端口号，打开新的浏览器页面进行访问，如下图所示：



使用“超级账户iotedgeadmin”登录“集群控制台”，用户名与密码一致，首次登录强制修改密码，此连接为内网地址，请保证电脑可以正常连接至内网，如下图所示：

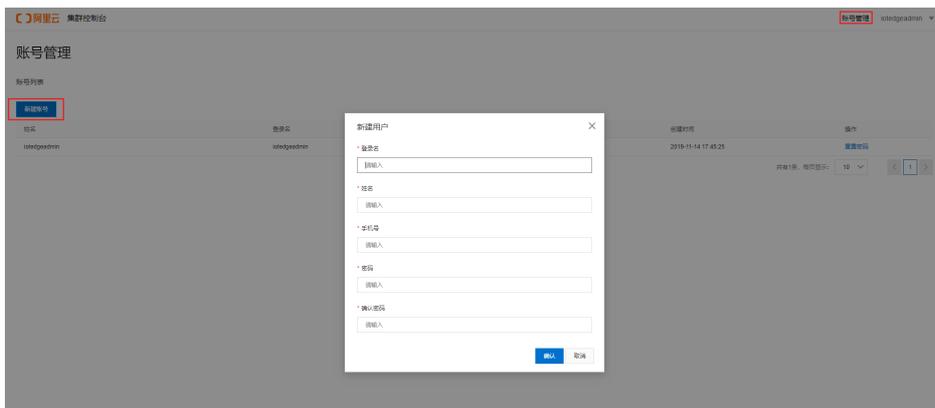


登录成功后，可单击部署应用的应用卡片，进入应用详情，如下图所示：



3.3用户管理

单击**账号管理**>**新建账号**，添加“集群用户”（用户名、密码、手机号），其中，手机号必填且唯一，并提示用户，手机号是系统之间免登的凭据，如下图所示：



如果您需要对边缘控制台的密码进行重置，可单击**组件管理**>**边缘用户中心**>**重置密码**功能，将修改后的边缘控制台密码重置为“超级账户iotedgeadmin”，如下图所示：



3.4应用监控

单击**运维管理**>**应用监控**，可查看部署在该集群中的应用名称、应用类型、免登地址等信息，单击页面中的**登录**，即可跳转至应用内部，如下图所示：



单击**应用监控**>**节点列表**可查看此应用的运行状态与端口信息，如下图所示：



单击应用监控>节点列表 > 容器管理可查看该应用的资源使用情况，如下图所示：



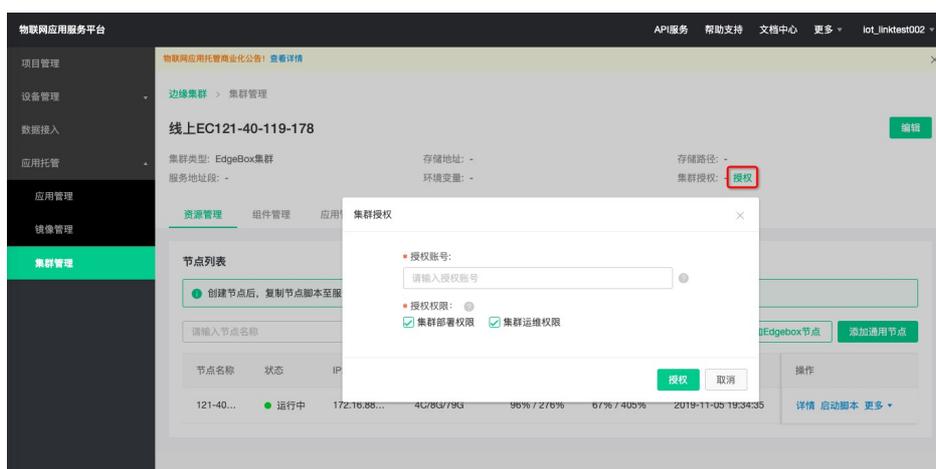
3.5 主机监控

单击运维管理>主机监控 可查看该集群下，已激活的主机资源配置详情，如下图所示：



3.6 集群授权

单击集群管理 > 授权 输入被授权方的用户账户名称，便可将创建的集群授权给对应的用户，如下图所示：

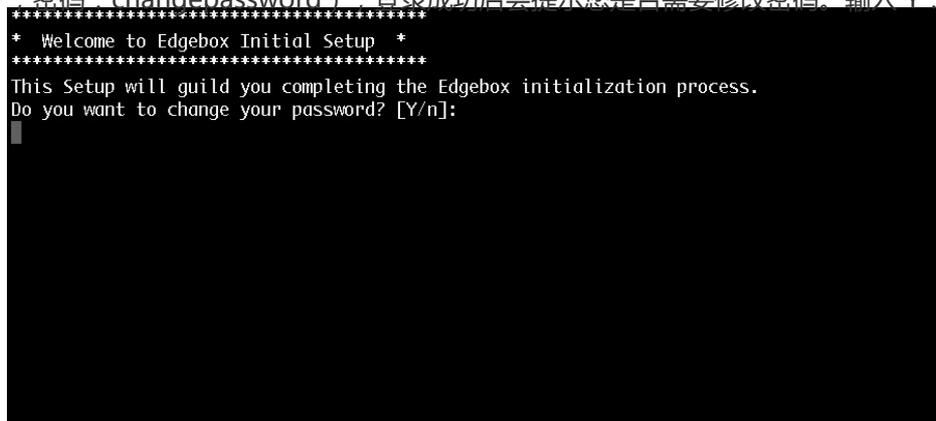


参数名称	参数说明
集群部署权限	支持被授权方可在该集群中进行其他应用部署。
集群运维权限	支持被授权方进行“创建节点”，以及节点的“删除”和“节点脚本”操作。集群编辑。

智能边缘一体机操作手册

1. 初始化系统

插入电源，将主机开机后，进入到欢迎页面，这时您需要使用默认的用户名与密码登录系统（用户：owner；密码：changepassword）。登录成功后会提示您是否需要修改密码。输入 Y：是，n：否，如下图所示：



设置成功后，提示您是否需要手动配置动态IP。输入 Y：是，n：否，如下图所示：

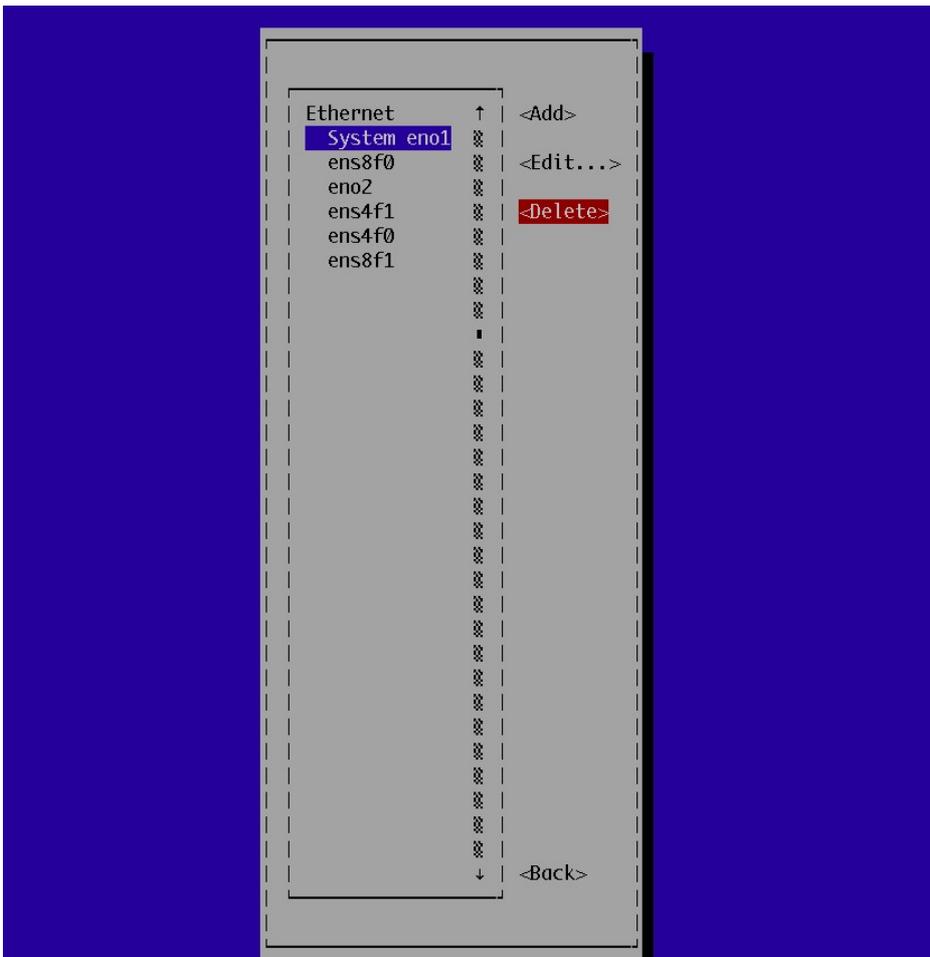
```
*****
* Welcome to Edgebox Initial Setup *
*****
This Setup will guide you completing the Edgebox initialization process.
Do you want to change your password? [Y/n]:
n
Merging home partition to root...
[sudo] password for owner:
Home partition is merged to root
Config network, do you want to use manual mode? [Y/n]:
y
```

若选择Y，进入手动命令行模式进行网络配置；否则，若选择n，跳转至CentOS自带的可视化网络配置页面，如下图所示：

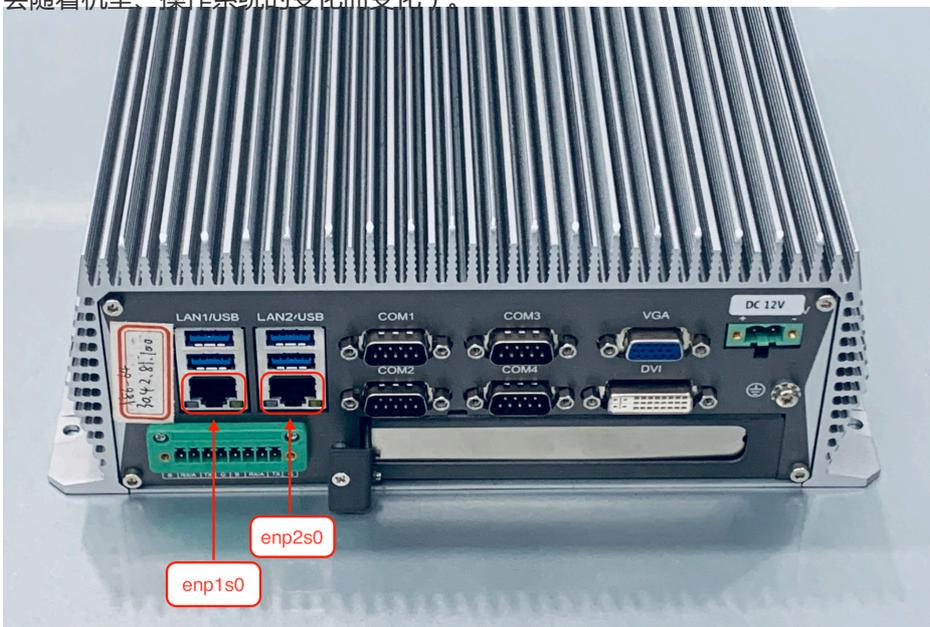


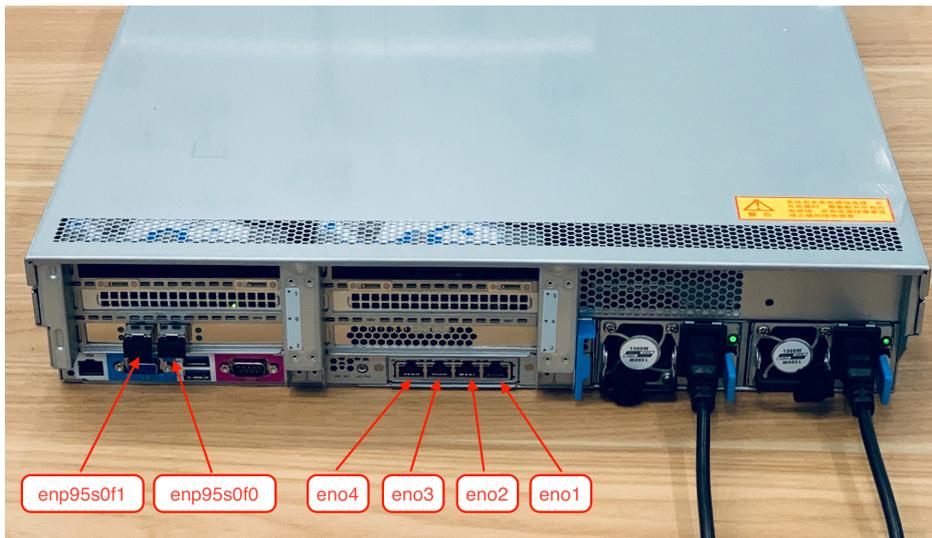
- Edit a connection：创建一个新的连接；
- Activate a connection：激活已配置的连接；
- Set system hostname；设置系统的主机名称；

选择Edit a connection跳转至可配置的节点（网口）页面。如下图所示：

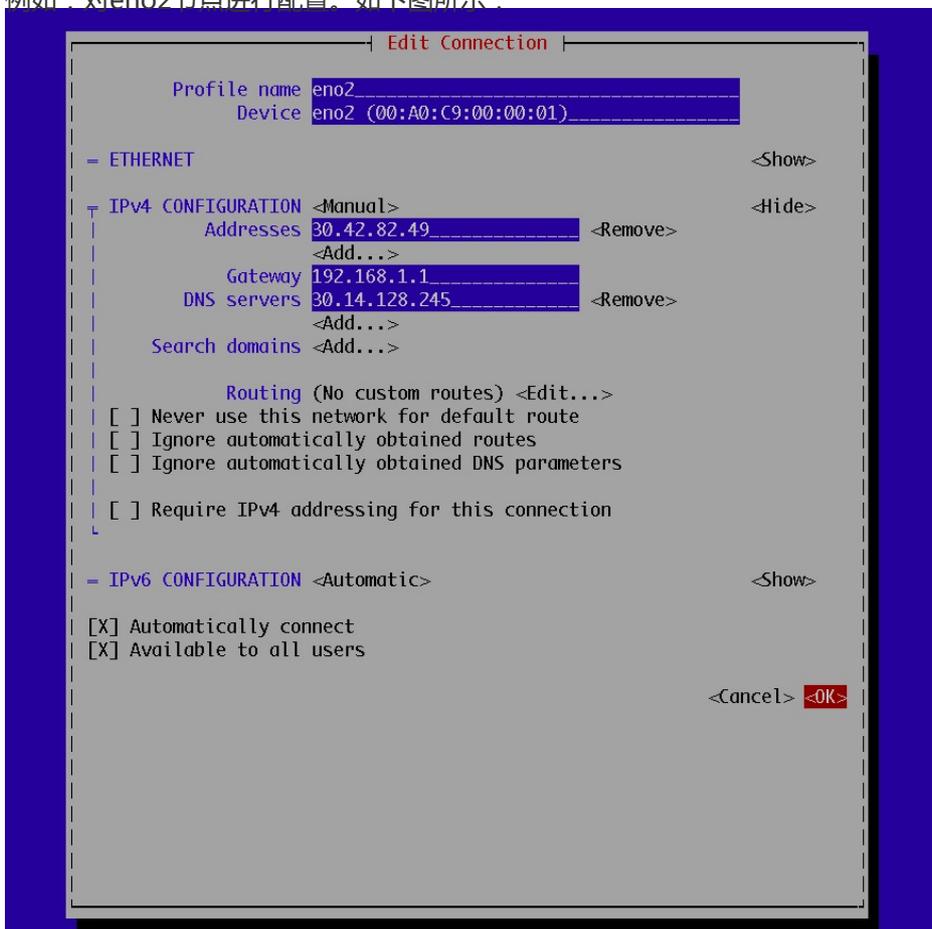


选择节点名称时，注意不同的机型，主机对应的网卡名称不同，典型的有如下示例（仅做参考，实际情况可能会随着机型、操作系统的变化而变化）。





例如：对eno2节点进行配置。如下图所示：

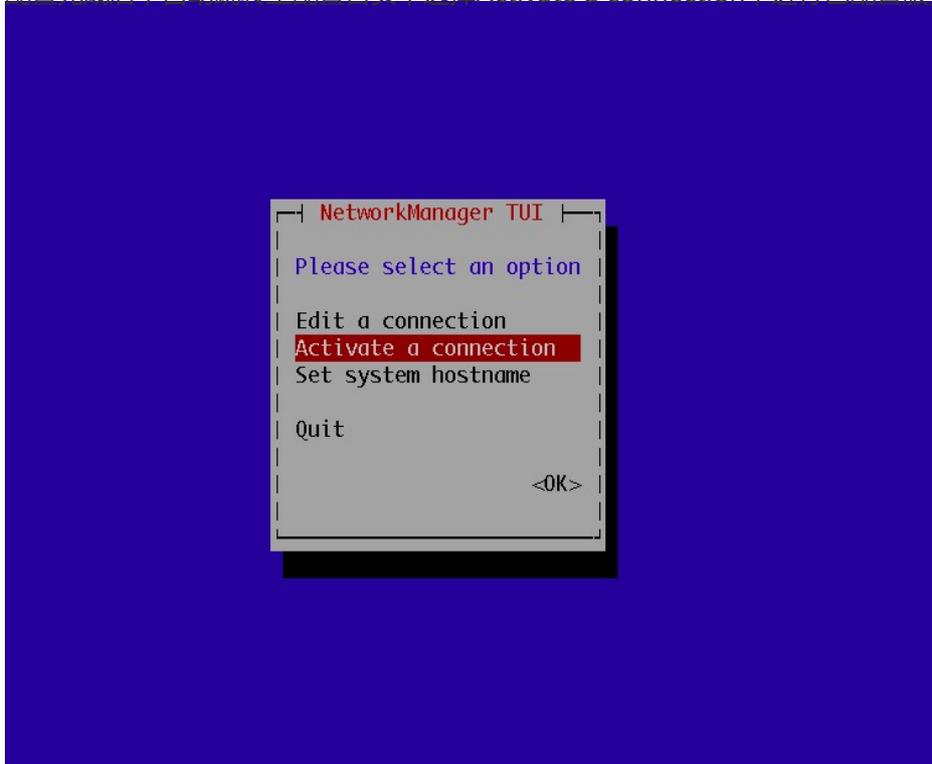


- Addresses：服务IP地址+子网掩码，格式为IP/掩码，如192.168.2.1/24，代表IP为192.168.2.1，子网掩码为255.255.255.0；
- Getway：网关路由；
- DNS Servers：DNS区域解析；
- Automatically connect：自动连接；
- Available to all users：适用于所有用户；

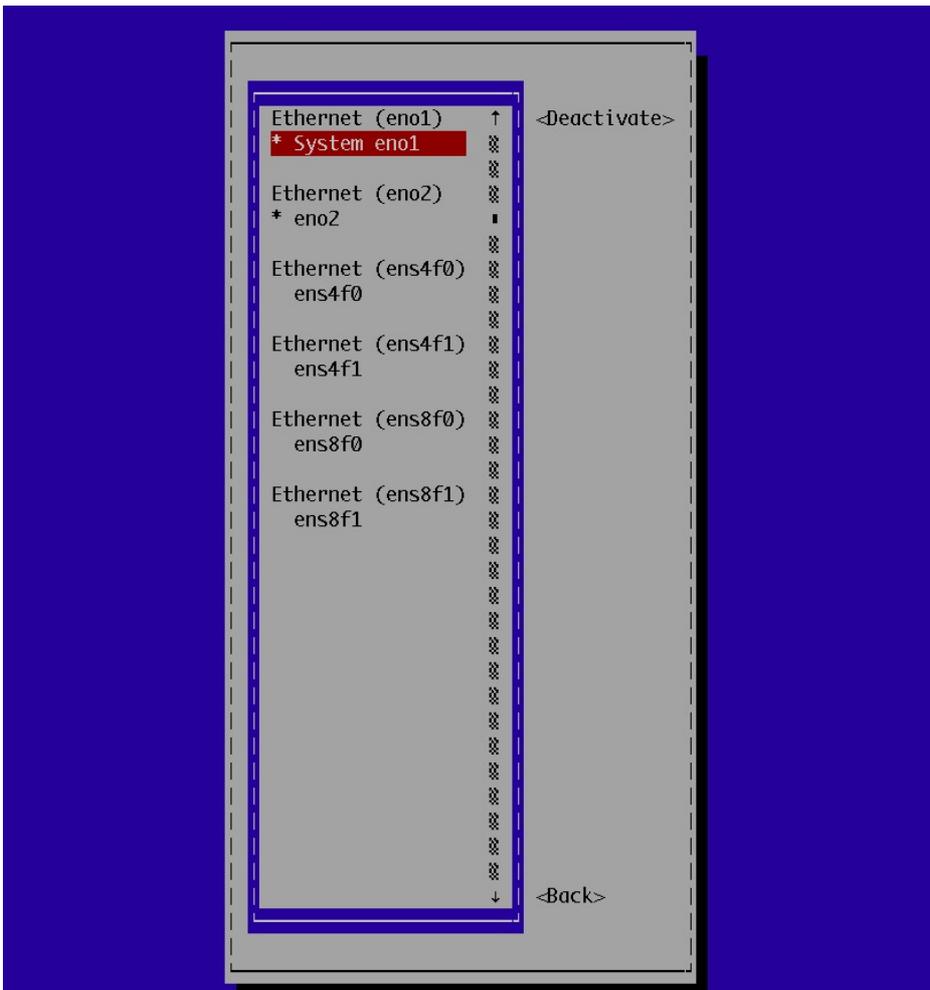
注意：

将光标标记至名称前，敲击空格进行选定，建议将Automatically connect与Available to all users选项进行勾选，“X”为选中态。

配置完成后，自动跳转至配置首页，选择Activate a connection，进行已配置服务IP激活，如下图所示：



“*” 标记为服务IP已经配置成功，可直接进行连接，如下图所示：



若选择n自动配置动态IP，将跳转至节点IP展示页面，eno1为动态获取的节点IP，eno2为上述手动配置的节点IP。如下图所示：

```

Home partition is merged to root
Config network, do you want to use manual mode? [Y/n]:
n
[sudo] password for owner:
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 30.42.82.67 netmask 255.255.255.128 broadcast 30.42.82.127
    inet6 fe80::2a0:c9ff:fe00:0 prefixlen 64 scopeid 0x20<link>
    ether 00:a0:c9:00:00:00 txqueuelen 1000 (Ethernet)
    RX packets 124034 bytes 26442825 (25.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1060 bytes 191367 (186.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device memory 0x9d120000-9d13ffff

eno2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 30.42.82.49 netmask 255.255.255.255 broadcast 30.42.82.49
    inet6 fe80::502a:2b52:3971:39ee prefixlen 64 scopeid 0x20<link>
    ether 00:a0:c9:00:00:01 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device memory 0x9d100000-9d11ffff

ens4f0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 70:57:bf:f9:a1:24 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens4f1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 70:57:bf:f9:a1:26 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens8f0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 3c:fd:fe:d2:3d:bc txqueuelen 1000 (Ethernet)

```

2. 激活设备

动态IP配置完成后，将提示您是否需要设置设备名称与设备激活码。输入名称后敲击回车键即可生效。如下图

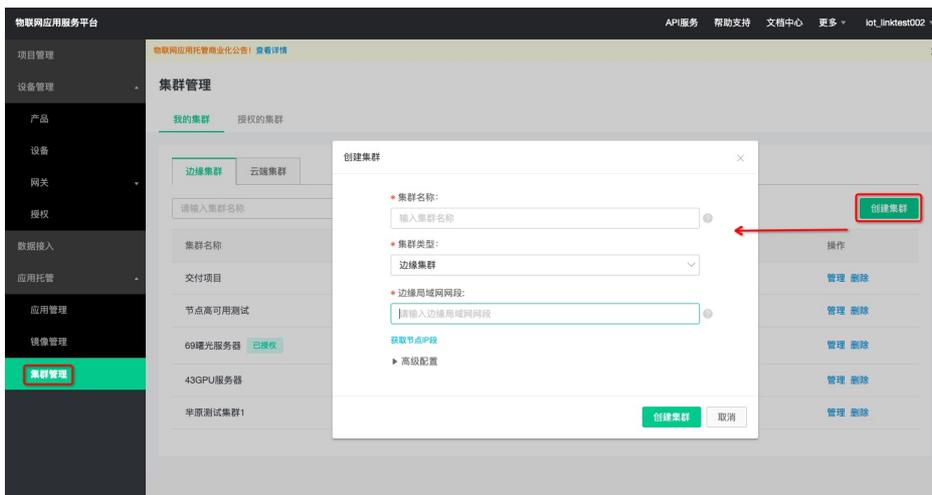
```

Is this network configuration OK? [Y/n]:
y
Setup user account...
Please input name for this device:
device01
Please input user bind code:

```

所示：

获取设备激活码，则需要先使用阿里云账号登录SI工作台在 **应用接入 > 集群管理** 页面选择集群类型为**智能边缘一体机集群**填写集群基本信息，如下图所示：



- 存储地址：NFS服务器地址。
- 存储路径：NFS Mount路径。
- 服务地址段：边缘可用来分配的边缘服务网段。

建议使用与当前边缘局域网段不同的子网，否则有发生IP冲突的可能性导致服务异常。例如当前主机所在网络为192.168.1.0/24；可在路由器中再添加另一个子网192.168.2.0/24专门用来分配服务VIP。

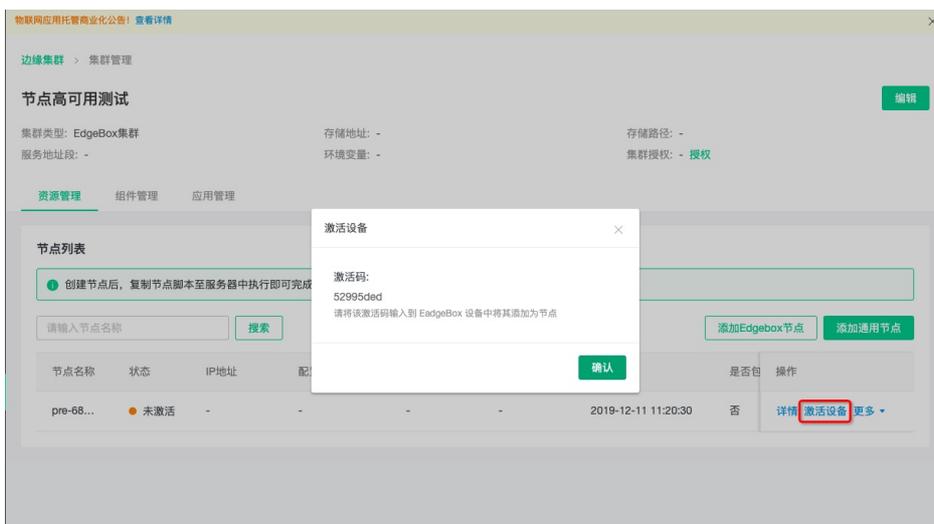
单击 **管理 > 资源管理 > 添加智能边缘一体机节点** 页面填写节点基本信息，如图所示：



节点名称：与集群名称不同，节点名称会被使用在K8S中，所以对命名有一定要求：只支持**数字、小写英文、短划线**，不能以短划线开头和结尾，长度限制4-30。

节点IP段：节点IP段为当前主机所在网段，需要用户提供以分配对应的Flannel Overlay服务网段。

选择创建成功的Edgebox节点，单击**激活设备**，可获取主机激活码。如图所示：



请使用通过激活设备，获取到的设备激活码输入到主机中。如下图所示：

```
Is this network configuration OK? [Y/n]:
y
Setup user account...
Please input name for this device:
device01
Please input user bind code:
52995ded
```

3.配置成功

激活码输入后，将进行安全系统校验，DPS的相关认证，设备激活的输出日志。当出现successful为激活成功。如下图所示：

```
Enable DPS
Optimizing system audit log
Start IOT Link Edge Services...
cp: cannot create regular file '/home/owner.tar.gz': Permission denied
tar: owner.tar.gz: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
Waiting for DPS activated...
DPS is activated
Start IOT Link Edge Services...
cp: cannot create regular file '/home/owner.tar.gz': Permission denied
tar: owner.tar.gz: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
Services installed !
Your system has been initialized successfully !
```

校验通过后，将跳转至激活成功页面。如下图所示：

```

*****
*   Welcome to Alibaba Cloud IoT Security Console   *
*****

[clish-info] clish execute : echo "Welcome `whoami` it is `date`"
Welcome owner it is Mon Dec 30 01:13:49 EST 2019
>

```

主机初始化时长大概5分钟，初始化完成后，节点状态将变成运行中。如下图所示：

节点列表

创建节点后，复制节点脚本至服务器中执行即可完成节点安装。

请输入节点名称

节点名称	状态	IP地址	配置	CPU	内存	更新时间	是否包	操作
node-1	运行中	30.42.82.77	8C/16G/50G	38% / 104%	26% / 109%	2019-12-26 14:43:20	否	详情 SSH 更多

线上集群部署的具体操作流程，请参考智能边缘一体机用户手册：

https://help.aliyun.com/document_detail/145504.html

Features

1. Product overview

Edge applications are applications that are deployed at the locations of the users. These applications are suitable for scenarios that require data to be processed in **real time** in a **secure** and **reliable** manner. For example, edge applications can be used for access control systems, building automation systems, and video algorithm applications.

EdgeBox provides a new deployment model for edge applications based on Kubernetes. Resources of edge hosts such as the CPU, memory, storage, and network are virtualized for scheduling, and applications are containerized for orchestration. You can use EdgeBox for lifecycle management and remote O&M of edge applications. Edgebox provides high security, high availability, reliable disaster recovery, and efficient resource utilization for the applications.

Multiple Edgeboxes can be virtualized into a single resource pool that includes resources such as the CPUs and the memory. Applications are packaged into containers and orchestrated within the

resource pool. At the same time, EdgeBox ensures the reliability and security of the applications that run in the resource pool.

2. Industry analysis

The current mainstream application deployment model often requires independent software vendors (ISVs) or users to provide one or more servers in the on-premises data center. This model has several problems:

Deployment and O&M

Without standardized infrastructure for edge applications, performing day-to-day tasks such as updates, monitoring, and remote O&M of applications becomes a challenge. Users are often unable to perform on-demand updates because ISVs often do not provide a dedicated channel for application updates. Furthermore, hosts deployed at the edge often do not have a public IP address and rarely allow remote access. This further complicates O&M and monitoring operations, and ISVs must perform such operations on-site. This approach is time-consuming and costly. Moreover, different applications may require different O&M strategies, which further increase the difficulty of maintaining the applications.

Disaster recovery and fault tolerance

Disaster recovery and fault tolerance operations for applications require a large amount of workload and training. EdgeBox solves this problem by providing a built-in KeepAlived component and middleware (such as MySQL) that creates multiple data replicas. This enables users to achieve high data and service availability in a distributed environment. EdgeBox also provides mechanisms to monitor applications and interact with containers.

Resource scheduling

ISVs often deploy different applications on different hosts to reduce interference from other applications and ensure the isolation of different applications. This inevitably leads to low resource utilization. Customers can choose to use infrastructure as a service (IaaS) solutions such as VMWare and OpenStack, but these solutions are costly and have high O&M requirements. Therefore, this solution is not suitable for small-scale edge applications. However, without such virtual infrastructures, it is also very difficult to scale applications and adjust resource utilization strategies based on actual demands.

Security

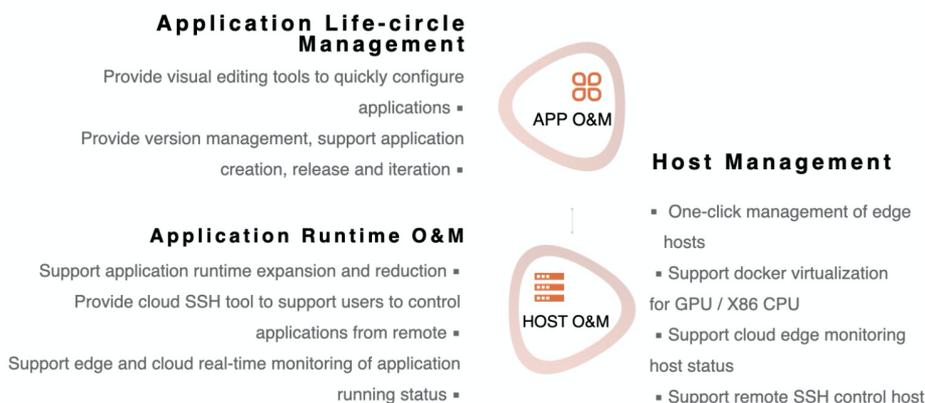
The mainstream model for deployment of edge applications introduces a series of security challenges for IT engineers and operators to tackle. Such challenges can include physically securing the hosts, responding to abnormal requests, detecting system looping holes, and performing timely updates. These security issues are often overlooked despite the fact that they are critical to the application deployment.

Integration and coordination

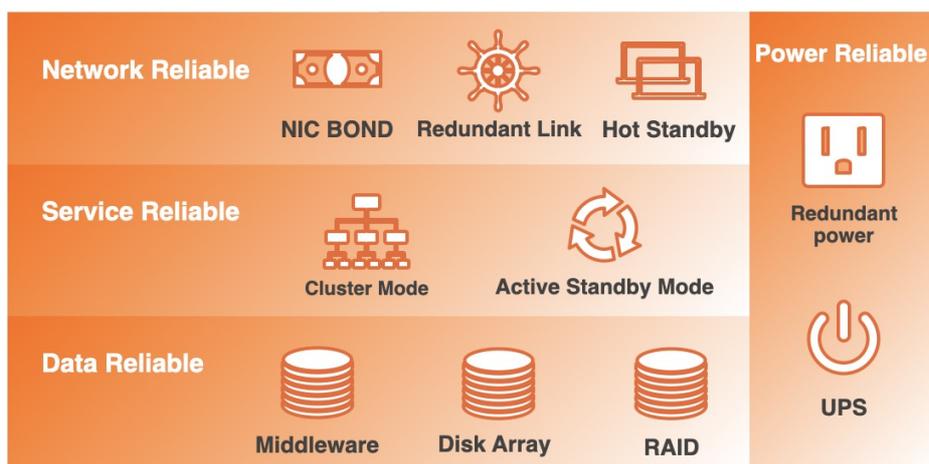
Companies with multiple branches often need to connect edge applications of different branches with the cloud platform of the headquarters. Under the mainstream model, edge-to-cloud requests can be achieved. However, cloud-to-edge communication is not possible and external users cannot use the edge applications. Edge applications of different branches are isolated because there are no dedicated communication channels or centralized account management.

3. Benefits

1. Efficient deployment and O&M



2. Reliable disaster recovery and high fault tolerance



3. High security



Use case

1. Background

The Sunac property services group is a company that serves over 400 residential complexes. To reduce operating costs and improve the experience of the residents, the company wants to transform the residential complexes by using AI technologies. To standardize the AI system for delivery, integration, and continuous O&M, the group came up with the idea "A closed-loop cloud interconnected to multiple closed-looped edges". To bring this idea to reality, the transformation process requires the following:

1. Independent edges: The system at the edge can perform basic functions without the need to be connected to the cloud. This prevents possible single-point failures from the

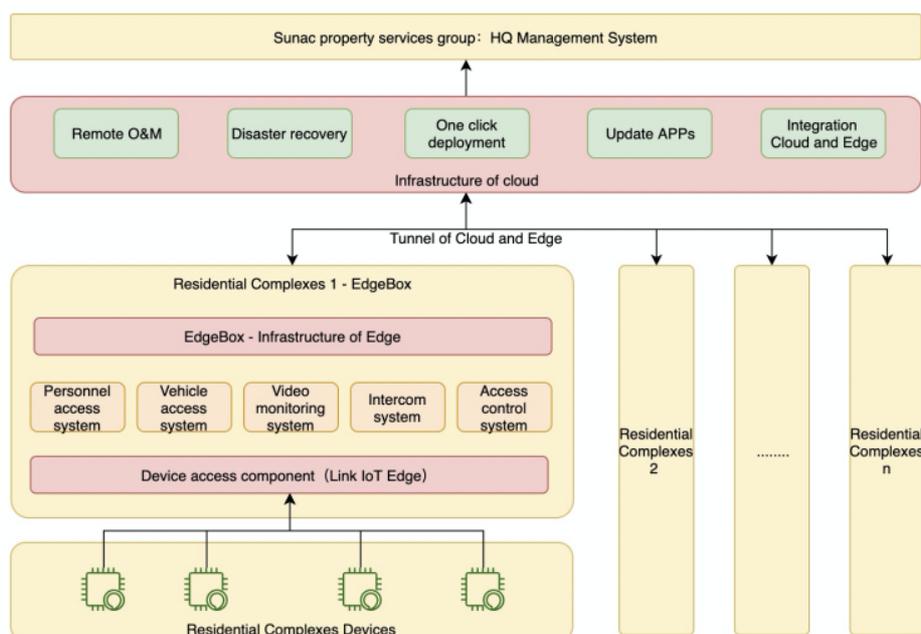
- headquarters and potential network instability.
2. Reliable edges: The system at the edge must support fault detection, data migration and data recovery to ensure the overall reliability of the service.
 3. Distributed replication: The overall system (including the subsystems) can be replicated and deployed to multiple residential complexes to reduce the deployment time.
 4. Remote O&M: The business system within each residential complex can be accessed remotely for monitoring, alerts, updates, and various emergency operations.

2. Solution

The Sunac property group has partnered with Alibaba Cloud IoT team to deploy their solution by using EdgeBox and Link IoT Edge. In the solution, applications can be independently managed at the edge and the company can dispatch and deploy applications from the cloud to the edge. This ensures high availability of edge applications and applications can be accessed, updated, and maintained over a remote connection. At the same time, the IoT team developed a dedicated service bus for information exchange so that the system is integrated from the cloud to the edge. By using Edgebox and implementing the solution together with Link IoT Edge, the Sunac property service group is able to quickly replicate and integrate the residence management system and greatly reduce the cost of building smart residential complexes.

The solution:

1. Migrate business applications to and subsequently host them on IoT Platform. These business applications include the pedestrian system, vehicle system, monitoring system, intercom system, and access control system.
2. Two EdgeBoxes are deployed at each residential complex. Each EdgeBox is installed with components for device access, high availability, data service, and threat detection.
3. During the deployment, applications are dispatched from the cloud to the EdgeBoxes and quickly replicated across different residential complexes.
4. To implement central management, the system is integrated with the internal management system of the Sunac property services group.



3. Results

By using Edgebox and implementing the solution together with Link IoT Edge, the Sunac property service group is able to quickly replicate and integrate the residence management system and greatly reduce the cost of building smart residential complexes.

智能边缘一体机产品介绍

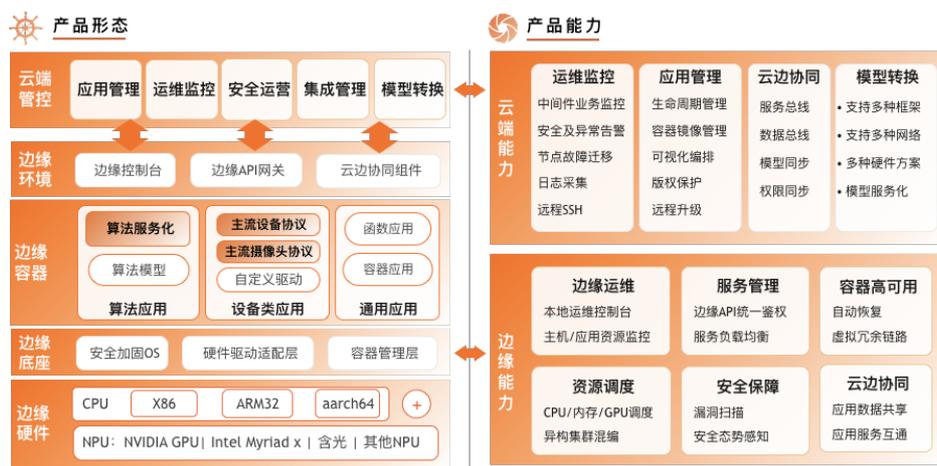
一、产品概要

边缘应用是指部署在用户现场的应用，常见于一些用户对数据处理**实时性**、**安全性**和运行**可靠性**要求比较高的场景下。如门禁系统、楼宇自动化BA系统、视频算法应用等。

EdgeBox是一种现场应用部署模式的变革，通过Kubernetes技术，将边缘主机的CPU、内存、存储、网络等资源虚拟化调度，以及应用的容器化编排，实现边缘应用的生命周期管理、安全运行支撑、高可用及容灾保障、以及远程运维能力，同时，有效提升了主机的资源利用率。

通俗地讲，EdgeBox将多个物理主机虚拟化成一个（CPU、内存等的）资源池，应用被包装成了一个个容器，并且被编排进总的资源池中，同时我们又在这个资源池里面建立了一套保障这些应用运行的能力。

产品架构如下：



二、行业现状

当前主流的边缘应用部署模式往往是为每一个应用提供商（ISV）在本地机房提供一台或多台服务器，主机可能是ISV提供，也有可能是客户自己提供。这种模式存在几个问题：

部署运维难：

由于没有统一的边缘应用的基础设施，传统的边缘应用部署常常会发现应用升级难、远程运维难、监控保障难。应用升级难，是由于ISV往往不会提供专门的升级链路给到用户，让用户可以按需升级。运维监控难，是指部署在边缘端之后，由于常常没有外网IP，也就没有链路实现远程对应用或者主机进行各种操作，于是ISV不得不现场解决，时效性差、成本还高。

不仅如此，每一个应用其部署运维都不尽相同，对于边缘侧部署多个应用的场景，运维IT人员往往束手无策。

容灾容错难：

传统的应用为了实现容灾容错，需要额外增加不少工作量，而且具备一定的部署运维门槛。EdgeBox通过提供具备高可用多副本能力的常用中间件（如MySQL），以及自带的KeepAlived组件实现数据和服务的多节点高可用。另一方面，EdgeBox还提供了一套应用健康状态检查机制和容器回复机制。

资源调度难：

边缘侧的应用提供商，为了保持自己应用的独立性，减少被其他应用的干扰，不同应用往往都要求被部署在不同主机上。这样势必导致资源利用率较低。但是利用IaaS虚拟化基础设施（如VMWare、OpenStack等），建设成本太高、运维要求也高。不符合小边缘的场景。另一方面，没有这种虚拟化的基础设施，应用的扩容缩容也很难实现，无法根据实际情况调整资源使用策略。

安全保障难：

边缘侧的主机如何加固？如何发现主机的安全风险态势，如某个IP定时发起一些异常的请求等？如何发现系统漏洞并及时打补丁。这些问题按照传统的方案解决，对IT和施工人员要求比较高。因此安全问题往往被忽视，但是却很致命。

云边集成难：

对于总部+分支站点的客户，往往需要将站点部署的本地边缘应用与总部控制的云端平台去做打通。传统模式下，往往只能实现边到云的服务请求，但是无法做到云到边缘的服务，即边缘应用无法提供服务给外部用户。此外，由于没有对边缘侧应用的数据和服务管理通道、以及登录账号的统一管理，部署到客户现场的应用常常无法互通，从而造成一个个信息孤岛。

三、产品优势

1. 产品优势：强大的部署、运维能力

应用生命周期管理

- 提供可视化编排工具，快速配置应用
- 提供版本管理，支持应用的创建、发布和迭代
- 在云端统一部署、删除、升级应用实例

应用运行时运维

- 支持应用的运行时扩容、缩容
- 提供云端SSH工具，支持用户从远程控制应用
- 支持边缘和云端实时监控应用的运行状况
- 日志采集工具自动注入，自动采集至云端进行分析



应用运维



主机运维

主机运维

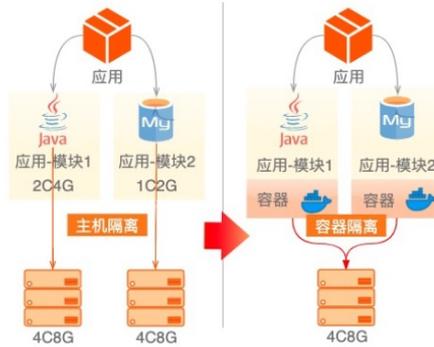
- 边缘主机一键纳管
- 支持GPU/X86 CPU虚拟化
- 支持云边监控主机状态
- 支持远程SSH控制主机

2. 产品优势：资源优化利用能力

- ### 1 资源超分
- 资源根据上下限设定
 - 保证应用可用
 - 防止过多挤占其他应用
 - 下限以上资源按需抢占



- ### 2 容器级隔离
- 应用间，或应用模块之间需要隔离
 - 传统模式是主机隔离，资源浪费
 - 采用容器级隔离，实现细粒度隔离



3. 产品优势：容灾容错和恢复能力

服务高可用

- 容器节点健康检查
- 容器节点自动按需重启
- 主机故障服务自动迁移
- Keepalived多副本保活

数据高可用

- 支持NAS共享存储
- 支持MySQL-HA
- 支持Redis-HA



4. 产品优势：产品安全能力



四、案例介绍

1. 背景和客户诉求

融创物业服务集团，服务400余个小区。为了降低运行成本、提升业主体验，需要对小区实施智能化改造。但是如何对智能化系统进行标准化交付集成和持续运维，集团提出了“边缘小闭环、云端大闭环”的系统建设思路。基于这个思路，进一步的对系统改造提出了如下需求：

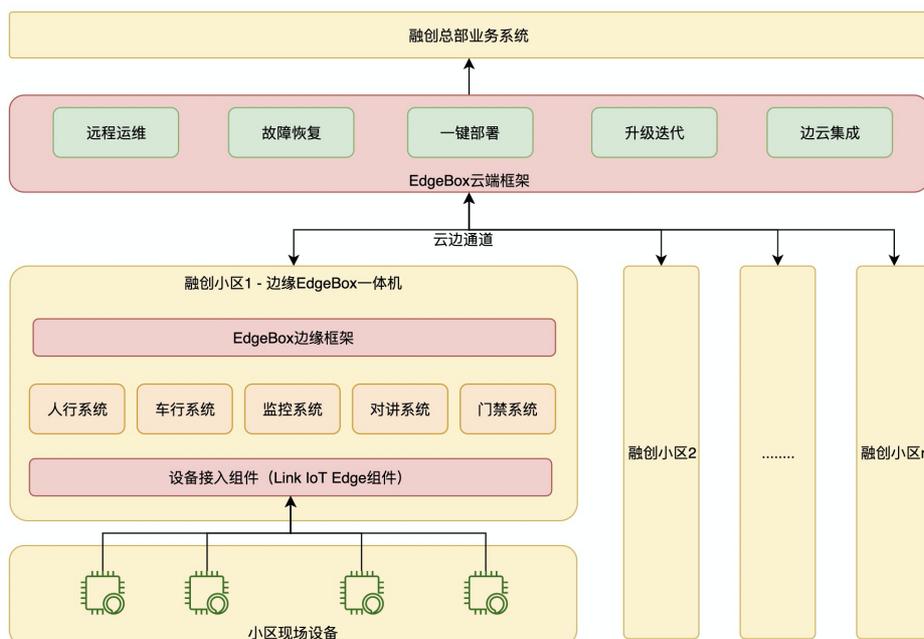
1. **边缘自治要求**：小区的业务系统能够在不连云的情况下，完成基础功能，以防总部单点失效和网络抖动；
2. **边缘可靠性要求**：能够为小区的业务系统提供故障发现、迁移、恢复的能力，提升可靠性；
3. **批量复制要求**：能够将对部署完成的业务系统（有多个子系统）批量复制到各个小区，缩短实施时间；
4. **远程运维要求**：能够对各个小区内的业务系统进行持续的监控、报警、升级迭代，并能远程访问进行各种应急操作；

2. 解决方案

通过边缘自治的应用管理能力和基于云到边的分发部署能力，为边缘应用提供高可用、可运维、可迭代的远程运维能力。同时提供云边协同组件，实现小区和总部的标准化云边系统集成，实现云端大闭环。通过实施基于“边缘应用管理平台”的智慧小区建设方案，帮助融创物业实现了小区系统的快速复制和快速集成，大大降低了小区智慧化改造成本。

具体来说：

- ①：将小区中用到的业务应用（包括人行系统、车行系统、监控系统、对讲系统、门禁系统），托管到边缘管理平台；
- ②：每个小区部署两台EdgeBox一体机，一体机内部自带“设备接入组件”、“高可用组件”、“边缘数据服务总线”、“安全感知组件”；
- ③：在部署小区时，一键从云端部署各个应用到边缘一体机，实现快速复制小区智能化方案；
- ④：在云端，通过统一的集成开放服务，对接融创总部管理系统；



3. 实施效果

通过实施基于“边缘应用管理平台”的智慧小区建设方案，帮助融创物业实现了小区系统的快速复制和快速集成，大大降低了小区智慧化改造成本。

Specification

1. Hardware specifications:

1. CPU: 40 vCPUs
2. Memory: 256 GB
3. Storage: 480 GB SSD, 24 TB (3 × 8 TB) HDD
4. GPU: 1 × T4
5. Network port: 2 × Gigabit Ethernet ports, 2 × 10 GB optical ports (with optical modules)
6. USB: 6
7. Operating temperature: 5 °C to 45 °C
8. Compact chassis
9. Weight : 48.5 LBS
10. Data eradication: N/A. Once deployed, edge appliance is part of customer' s private deployment along with their on cloud control-plane functionalities. Therefore any data

eradication would be customer' s responsibility.

11. Encryption : TPM Module embedded.



2. Features:

1. Supports lifecycle management and remote operations & maintenance (O&M) for container-based edge applications.
2. Provides a graphical console to manage applications and a centralized account management system.
3. Coordinates the cloud and the edge to synchronize data, services, accounts, and devices.
4. Protects software copyrights by using the Trusted Execution Environment (TEE) technology.
5. Supports communication protocols such as OPC UA, M-Bus, Modbus, KNX, BACnet, and SNMP for device access.