

微服务器操作指南

V1.0.3

包装清单



主机



电源线



SATA 数据线



SATA 电源线（选配）

重要提醒

微服务器高级功能如：防火墙、网络规则、路由策略、vlan 等，在未能充分理解，且不确认是否有修改需求时，请勿尝试修改，尤其是防火墙里面的设置，设置不当可能造成微服务器无法正常使用

虚拟主机如果为 linux，请删除默认的 e1000e 网卡，创建 e1000 网卡

千万不能把微服务器的“上网配置”里的 wan，和“局域网设置”里的 lan，两个 IP 设置为一致，会导致 IP 冲突，微服务器变砖

虚拟机可以访问 U 盘，若是 windows 系统，需要安装 usb3.0 驱动，且将 USB 接入主机

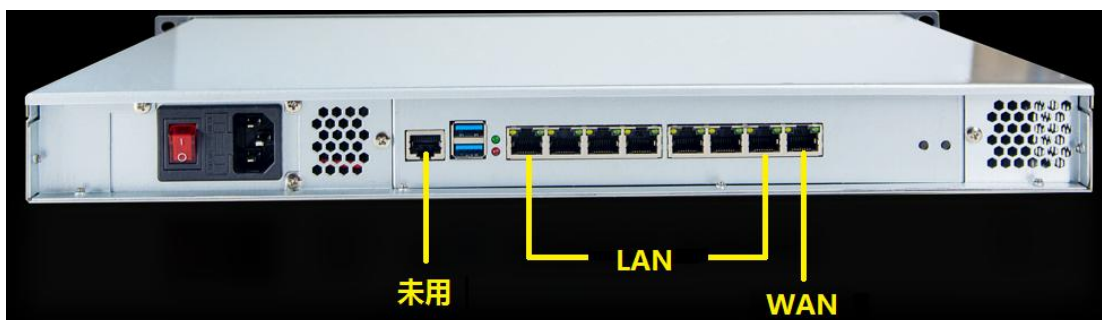
重要更新

- 虚拟机可以开机自启
- 可以创建多个虚拟机，自由分配内存大小，并可以增加虚拟磁盘
- 支持用 U 盘直接启动虚拟机
- 支持划分 vlan
- 支持设置多 wan 口和策略路由、静态路由
- 支持从局域网访问微服务器 lan 侧设备（参见防火墙设置，wan 域规则）
- 增加实时连接监控，在线拉黑 IP
- 支持建立网络访问规则，阻止各种非法访问（参见网络规则）

目录

一、	硬件和外观和硬盘安装	5
二、	状态	7
三、	基本设置.....	7
1.	设置上网方式	7
2.	设置 lan	8
3.	划分 Vlan	9
四、	公网 IP 管理.....	11
1.	映射	12
2.	DMZ.....	12
3.	透传	13
五、	虚拟机	14
1.	磁盘管理	14
2.	创建虚拟机	15
3.	虚拟机管理	17
4.	用 U 盘启动虚拟机.....	18
六、	高级功能.....	19
1.	防火墙设置	19
2.	网络监控	21
3.	网络规则	22
4.	路由策略设置	23
5.	端口映射	24

一、硬件和外观和硬盘安装



从左至右：

- 控制台（未用）
- USB 口*2，可用
- 网口，根据购买型号不同，有 4 口、6 口和 8 口的
 - 所有型号：**最右侧网口为默认的 wan 口**，其他为 lan 口（可以在管理页面修改为任意口，也可以增加多个 wan 口）

型号	入门版	标准版	专业版	至尊版
CPU	Intel Celeron J1900	Intel Celeron 3865U	I5-2520	i7-6500U
内存	8G	8G	8G	16G
SATA3.0	1	1	2	2
1000M 网口 (兼容 100M)	4	6	8	6
尺寸：	48.5*41*4.5 (cm)			
供电：	220V 交流			
功耗：	无虚拟机约为 16w，开虚拟机约为 25w			
管理页面：	默认为 192.168.148.1（可修改）			
管理密码：	默认为 888888			

修改密码:

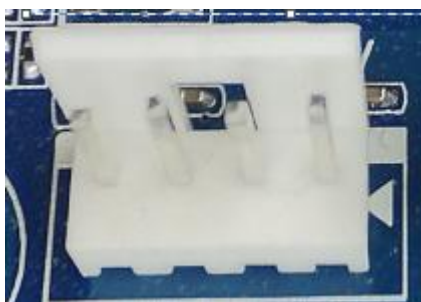


硬盘安装:

因硬盘在运输过程中容易损坏，微服务器出厂无硬盘，产品价格为无盘价



SATA 数据线接口



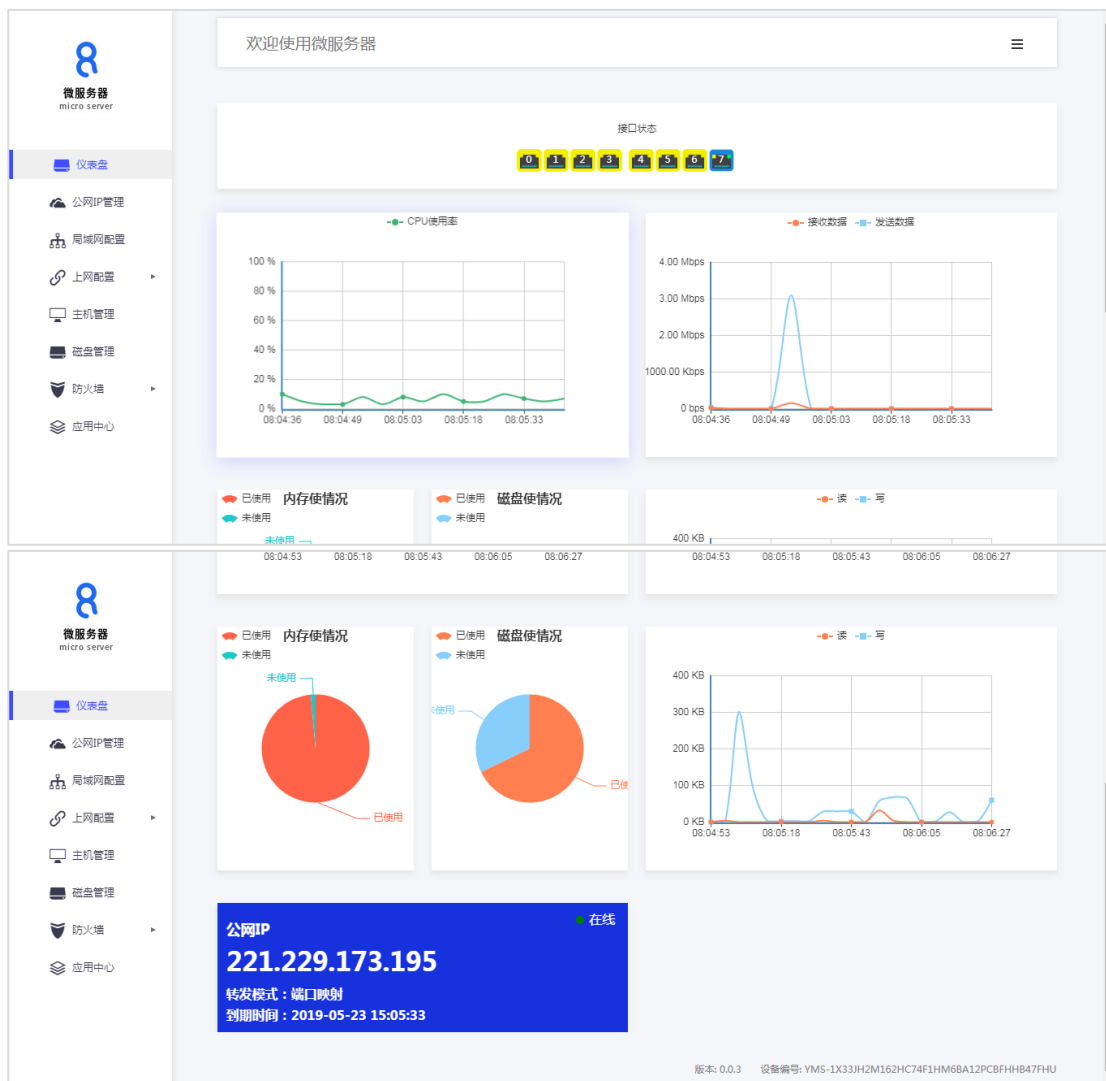
SATA 电源线接口 (或用电源上的接口线)



硬盘支架

二、 状态

进入微服务器，默认显示仪表盘，显示 CPU、网络接口、硬盘、内存、公网 IP 等实时使用情况：



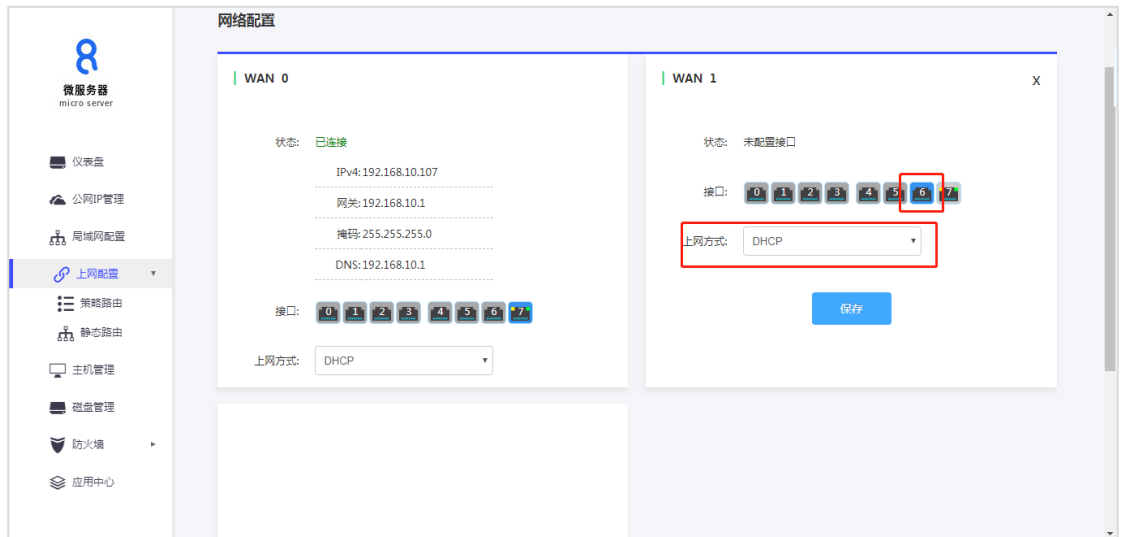
三、 基本设置

1. 设置上网方式

- 点击“上网配置”，可以配置 wan 口，默认情况下，微服务器的 eth7 为 wan 口，使用 DHCP 方式上网，可以在这里修改。支持 pppoe、DHCP 和静态 IP 三种方式

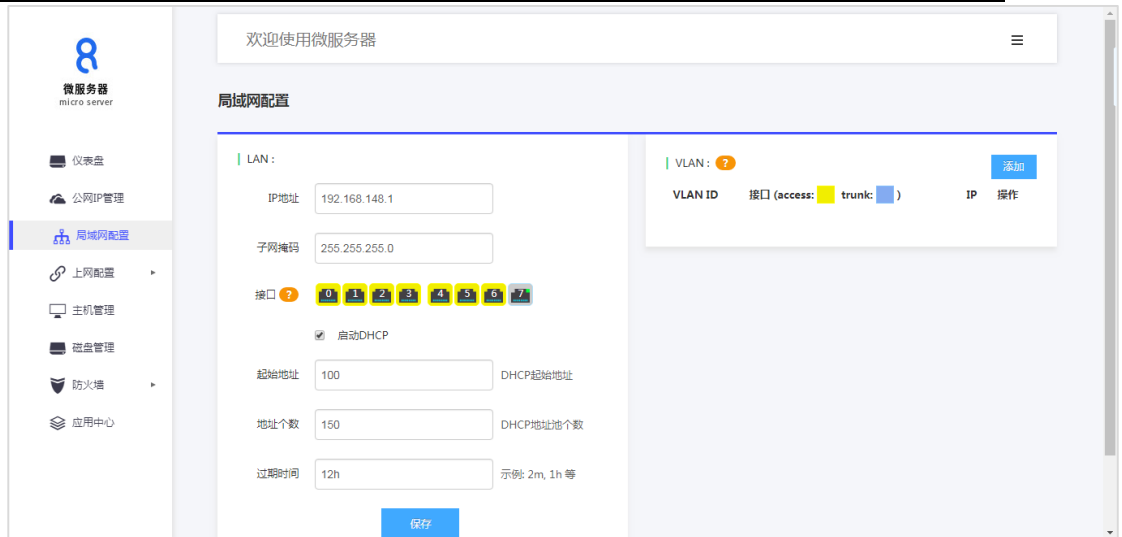


- 除了默认 wan 口之外，还可以增加 wan 口，点击添加 wan1，然后设置使用的接口和上网方式即可



2. 设置 lan

点击“局域网配置”，设置微服务器的 lan 口地址，和普通路由的设置相似，在这里可以设置微服务器的局域网地址和子网掩码，以及 DHCP 启用方式：



- 在这里可以看到各个网口的连接情况，已经连接上的网口，会显示 lan 和 wan 两个指示灯且不停闪烁（有流量通过的情况）

3. 划分 Vlan

若不理解 Vlan 概念者请先自行百度，若仍然无法理解、且没有特殊需求的，建议不要改动本节设置

点击“局域网配置”中的 Vlan 一栏里的添加，可以建立 Vlan:

VLAN

VLAN ID:

access接口 ? : 0 1 2 3 4 5 6 7

trunk接口 ? : 0 1 2 3 4 5 6 7

IP:

子网掩码:

[DHCP配置选项](#)

[防火墙配置](#)

- Access 接口：选中的网口只能属于一个 Vlan
- Trunk 接口：选中的网口可以属于多个 Vlan



注意: trunk 接口一般是给交换机等设备使用的, 普通电脑系统无法直接使用, 感兴趣的可以阅读以下文章:

<https://www.cnblogs.com/weiyikang/p/4945914.html>

https://blog.csdn.net/weixin_40759186/article/details/80926044

https://blog.csdn.net/wang_xya/article/details/38256595

- DHCP 和防火墙 zone:

VLAN

子网掩码: 255.255.255.0

DHCP配置选项

启动DHCP

起始地址: 100

地址个数: 150

过期时间: 12h 示例: 2m, 1h 等

防火墙配置

防火墙Zone: lan (selected), wan, 新建zone

DHCP 和 lan 设置相同

防火墙 zone 默认为 lan，如果有特殊需求的，可以新建 zone，但是后面的防火墙设置规则需要重新做，不推荐普通用户使用

四、 公网 IP 管理

微服务器
micro server

仪表盘

公网IP管理

局域网配置

上网配置

主机管理

磁盘管理

防火墙

应用中心

欢迎使用微服务器

公网IP管理

公网IP: 221.180.172.101 已连接

IP区域: 江苏

带宽: 100M共享

到期日期: 2019-05-23 15:05:33

转发模式: 透传模式 | DMZ | 映射模式

将端口映射到内网的服务器端口:

#	公网端口	协议	内网IP	端口	备注	操作
1	52309	tcp	192.168.148.101	3389		删除

- 上面可以查看公网 IP 地址，以及所属节点名称，带宽和服务期限
- 下方可以选择三种模式，其中端口映射和 DMZ 和普通路由的相同，透传模式为独有

1. 映射

首先要启用端口映射方式，然后点添加：



- **公网端口：** 即从外网用这个端口来访问，如：1.1.1.1: 81，后面的 81 即为公网端口（外部端口）
- **协议：** 一般为 TCP，若确认其为 UDP，则选 UDP
- **内部 IP：** 本地服务器的 IP（内部端口），如果是要映射到微服务器自身，在这填微服务器的 lan 口 IP；如果是虚拟机，填虚拟机的 IP
- **内网端口：** 本地服务器使用的端口
- **备注：** 可填项，方便管理
- 可以添加多个端口映射规则，可以有多个外部端口映射到同一个内部端口（包括同一个内网 IP 的同一个内网端口），但外部端口不能重复
- 可以**按范围映射端口**：如外部端口范围：10000—10010，映射到内网 IP 的数量相同（本例为 11 个）的端口范围（如 5000—5010），这样在做 FTP 被动端口映射等需要映射多个端口时，可以一次性设置好

注：这里的端口映射和防火墙的端口映射是两个不同功能，这里是特指与公网 IP 对应的端口映射，而防火墙的端口映射是指微服务器 wan 或 lan 的 IP 访问时的端口映射（类似于普通路由器的端口映射）

若要远程管理微服务器，即可按上图设置（上图用公网 IP:81 可访问）

2. DMZ

同样先启用 DMZ，DMZ 的意思：将所有公网访问转到指定的内网 IP 上（可以是连接到微服务器的设备，也可以是虚拟机），在这里填写上 IP 地址即可从外

网用公网 IP 访问到这台设备或虚拟机

转发模式：

透传模式 **DMZ** 映射模式

DMZ指向内网的服务器IP:

192.168.148.100

3. 透传

该模式较为复杂，简单来说，就是将公网 IP 直接配置在指定网口所连接的设备或按图上的方法配置 IP 的设备上，如果要透传到设备，设备连接到指定网口然后开启自动获取 IP 即可；如果要透传到虚拟机，虚拟机配置为公网 IP

转发模式：

透传模式 DMZ 映射模式

可以指定端口

请将服务器网络配置成DHCP并连接至以下网络接口：

0 1 2 3 4 5 6 7

服务器将获取到以下配置(也可以将此配置直接配置到服务器):

IPv4: 192.155.162.1

网关: 192.168.148.1

子网掩码: 255.255.255.255

DNS: 192.168.148.1

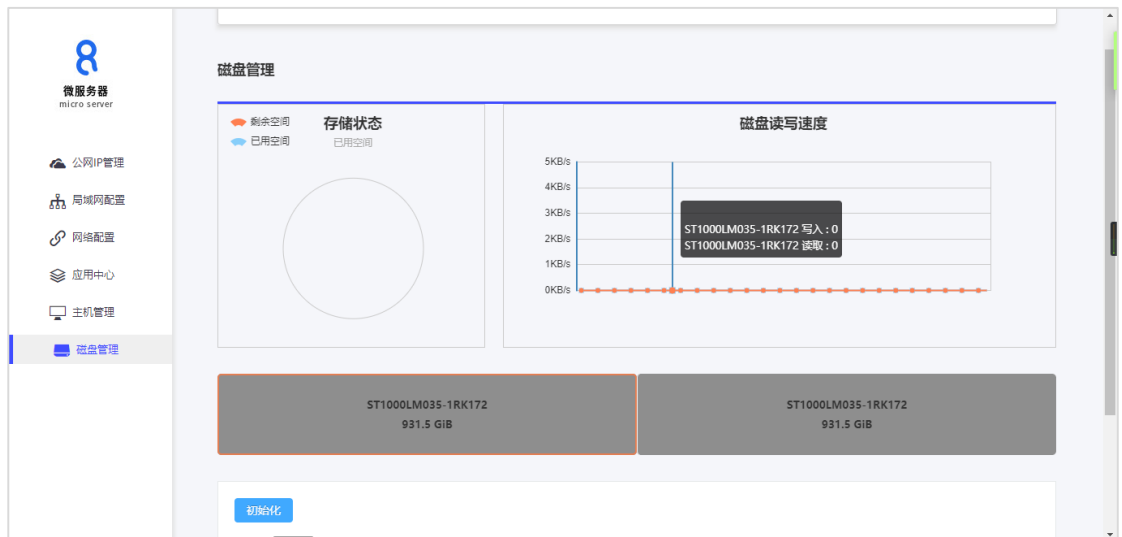
五、 虚拟机

1. 磁盘管理

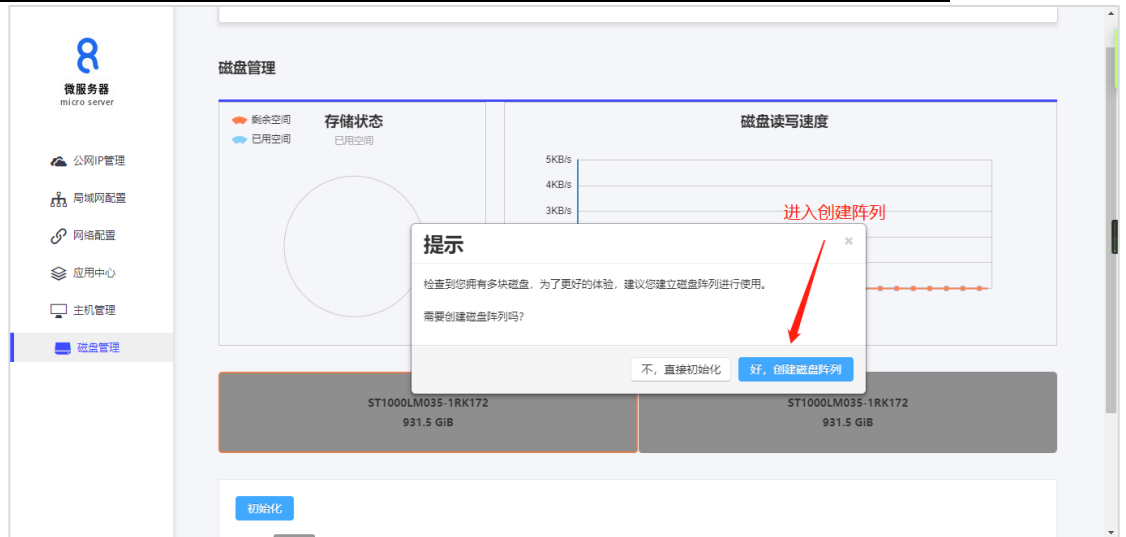
只有安装磁盘后，才可以安装虚拟机和应用，在“磁盘管理”一栏，可以看到当前磁盘的基本情况和实时读写速度



- 微服务器除了常规单硬盘模式外，还支持 raid0 和 raid1 阵列，目前最多可以上 2 块硬盘，最大容量 4T
- 使用磁盘前，需要先初始化，如果只有单硬盘，无法创建阵列，直接初始化后即可使用



- 阵列在初始化时建立，raid1 阵列在磁盘出问题时，可以移除问题磁盘，然后替换新硬盘，重新初始化并加入阵列即可



- 请根据自己实际情况规划阵列, 一般情况下, 若没有重要数据, 可以不做阵列; 如果有重要数据, 又采用固态硬盘的, 建议做 raid1

2. 创建虚拟机

展开“主机管理”一栏, 点击创建



- **主机名称:** 随意填写, 不要填写特殊字符
- **存储空间:** 在右侧显示的可用空间范围内, 设置存储空间; 该空间设置后并不是马上就占用设置的大小, 而是随着使用增长, 且一旦设置好之后, 无法再更改, 所以可以在可用范围内, 适当设大一点
- **虚拟机的启动和安装方式:** 支持从 U 盘直接读取 ISO 文件, 或者直接使用整个 U 盘作为启动媒体, 注意, 只能选择其中一项

创建好之后, 点右侧的“配置”

win	关闭	1	1024	开机 控制台 配置 克隆 删除
-----	----	---	------	------------------------

控制台 **配置** 开机 电源 ▾ USB设备 ▾ 快照

主机win

自启动

- CPUS
- 内存**
- 磁盘
- CDROM
- 网络
- USB

启动

自动启动虚拟机

CPUs

CPU总数 4

当前分配 1

cpu核心

cpu线程

内存

控制台 **配置** 开机 电源 ▾ USB设备 ▾ 快照

内存

推荐内存 2048MiB

分配内存(MiB)

磁盘

磁盘编号	大小	操作
磁盘1	30G	删除
新磁盘	<input type="text" value="50"/>	新建磁盘

CDROM

磁盘镜像(iso)



- **自动启动虚拟机:** 需要开机自启动的, 勾上
- **CPU 数量:** 在这里设置 CPU 核心和线程数量, 可以超过 CPU 物理核心和线程数
- **内存:** 因微服务器本身要使用一定内存, 推荐留出至少 1G。请注意: 同时运行的虚拟机所占用的内存总数, 不能高于 8G, 否则后面的虚拟机开不了机
- **磁盘:** 刚才分配的磁盘空间不可修改, 但可以用新增的方式, 再加一个虚拟磁盘上去 (所有虚拟磁盘的大小需小于可用物理空间)
- **CDROM:** 前面所选的 ISO 镜像, 与 USB 方式只能二选一
- **网络:** 在这里管理虚拟机里的网卡, 默认为 e1000e, 千 M 网卡, 但需注意: CENTOS7 以上的版本不支持 e1000e, 需要删除后创建一块 e1000 的千 M 网卡, 可同时指定其 mac 地址:



- **USB 设备模式:** 默认为 3.0

3. 虚拟机管理

一切就绪后, 就可以开机并安装系统了, 与常见虚拟机系统创建虚拟机的方式相似,

系统安装完成之后，需要对虚拟机关闭电源再启动，才能进入安装好的系统（否则还是进入 U 盘或者 ISO）

状态	CPUs	内存	操作
正在运行	4	6144	关机 关闭电源 控制台 配置 克隆 删除

开机之后，点击控制台，弹出网页控制台，功能比较丰富，主要功能见下图：



- 关机、暂停、电源等功能，与常见虚拟机系统类似
- 截屏：将屏幕保存为一张.ppm 格式的文件，可以下载到本地，用看图软件查看
- **USB 设备**：可以将 USB 设备实时加入、移除出虚拟机。虚拟机可以访问 U 盘，若是 windows 系统，需要安装 usb3.0 驱动，且将 USB 接入主机
- 快照：建立一份系统快照来备份，方便以后恢复
- 克隆：克隆一个虚拟机，包括其所有配置和文件，克隆需要在虚拟机关机的情况下进行；克隆和快照的区别：克隆相当于是对虚拟机进行复制，而快照是对虚拟机进行实时备份

4. 用 U 盘启动虚拟机

如果遇到系统崩溃、忘记密码等原因，无法进入虚拟机系统，可以准备一个启动 U 盘，能进入 pe 系统，然后启动到 pe 对虚拟机资料进行备份，具体办法：

- 1) 制作启动 U 盘（请自行百度）
- 2) **虚拟机关机**，请注意，一定要在关机的情况下进行后续操作才有效



3) 点击“配置”，然后把 USB 盘加入虚拟机系统



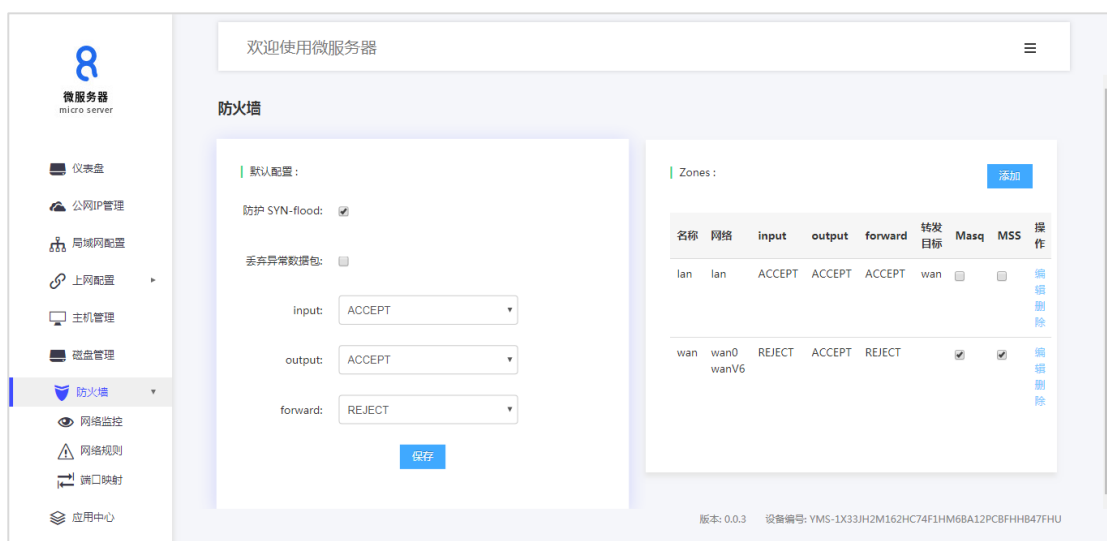
4) 虚拟机开机，就可以进入 U 盘系统了，如果虚拟机分配的内存低于 2G，请选择启动 WIN2003PE



六、高级功能

1. 防火墙设置

这里的防火墙设置，是类似于普通路由器的防火墙设置，仅作用于微服务器设备本身，和公网固定 IP 的关系不大



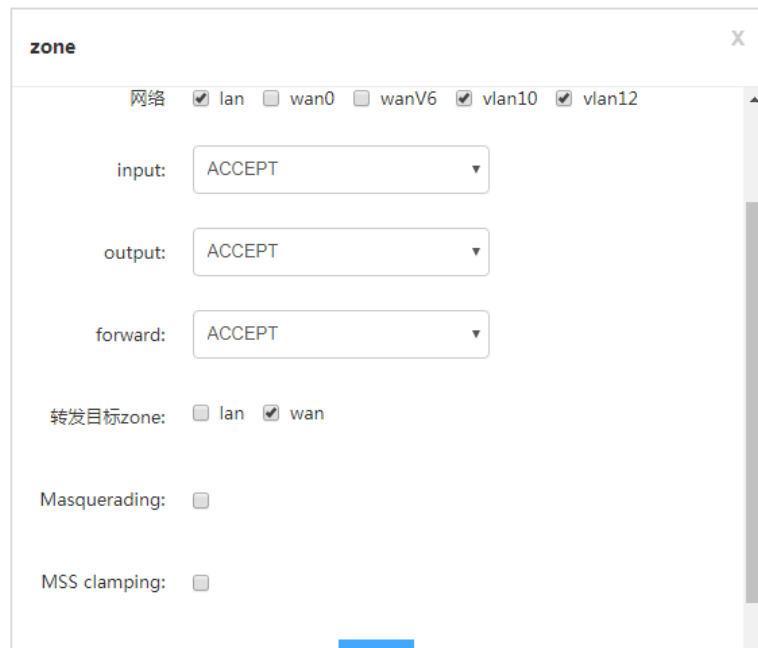
- 默认配置：不在右侧 zones 规则内的所有数据包的传输策略，默认情况下：
 - 防护 SYN-flood：防止 SYN 洪水攻击，默认不选中，用户可选中

- 丢弃异常数据包：默认不选中，用户可选中
- Input: accept, 接受；所有直接访问微服务器的数据包，都接受
- Output: accept, 接受；所有微服务器出站的数据包，都放行
- forward: reject, 阻止；所有需要微服务器转发的数据包，拒绝

系统已经自动建立了 lan 和 wan 的默认规则，不在这两个域内的访问规则。若用户未建立除 lan、wan 以外的 zone，则本项设置无意义

➤ Zones: 默认已经建立了 lan 和 wan 的传输规则

- lan 默认规则:



zone

网络 lan wan0 wanV6 vlan10 vlan12

input: ACCEPT

output: ACCEPT

forward: ACCEPT

转发目标zone: lan wan

Masquerading:

MSS clamping:

- lan 域默认包括 lan 和用户建立的 vlan（上述 Vlan10 和 12 在建立时被选择为 lan 域）
- Input: 所有从 lan 域访问微服务器的数据包，默认接受，如果不接受，所有微服务器的内网设备和虚拟机均无法访问微服务器!!!
- Output: 所有从微服务器发往 lan 域的数据包，默认放行，如果不放行，微服务器无法访问内网设备和虚拟机，那么相应的，内网设备和虚拟机收不到微服务器的返回数据，也就无法互相访问了
- Forward: 所有 lan 域需要转发的数据包，默认放行，如果不放行，微服务器的内网设备和虚拟机将无法上外网
- 转发目标 zone: 默认转发往 wan 域
- Masquerading: SNAT 的特殊方式，lan 域默认不选中
- MSS clamping: MTU 钳制，lan 域默认不选中

- wan 默认规则:

zone

网络 lan wan0 wanV6 vlan10 vlan12

input: REJECT

output: ACCEPT

forward: REJECT

转发目标zone: lan wan

Masquerading:

MSS clamping:

- 网络：默认包括 wan0（系统默认 wan）和 wanv6（IPV6），如果有建立其他 wan 口，也会出现在这里
- Input: 从 wan 域直接访问微服务器的数据包，如通过 wan 口 IP 直接访问微服务器，默认为阻止，如果打开，就可以通过微服务器的 wan 口 IP 直接访问到微服务器，慎用
- Output: 从微服务器出站的数据包，默认为放行
- Forward: wan 域需要转发的数据包，默认为阻止，如果打开，就可以在局域网内直接访问到微服务器 lan 侧的设备，如虚拟机，慎用
- 转发目标 zone: 默认不转发
- Masquerading: SNAT 的特殊方式，wan 域必须选中，不然微服务器 lan 侧的设备和虚拟机无法上外网
- MSS clamping: MTU 钳制，wan 域默认为选中

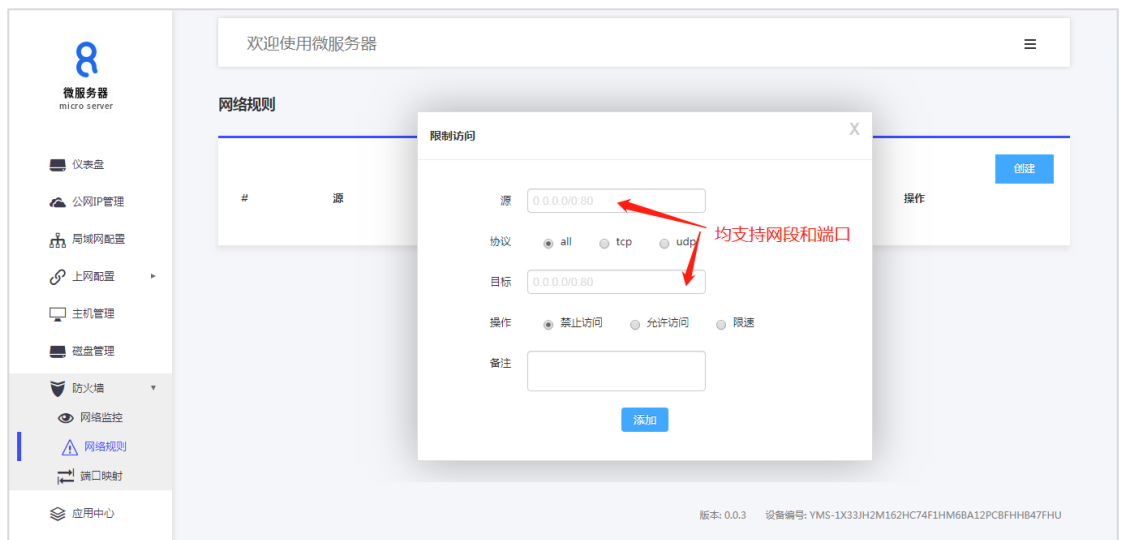
2. 网络监控

查看实时连接和流量，可以点击 IP 后面的小红 X，对疑似异常的连接进行阻止



3. 网络规则

可以建立网络访问规则，禁止或允许访问某些 IP，支持指定 IP 段范围和端口
如果要公网固定 IP 的访问进行限制，可以在这里进行设置



- 源和目标：可以全填或只填其一
 - 支持单个 IP，如：192.168.148.1
 - 支持 IP 范围，如：192.168.148.0/24，即子网掩码为 255.255.255.0 的整个段，192.168.148.1—254
 - 协议可以同时支持 tcp 和 udp
 - 支持指定单个端口或端口范围，格式为：192.168.1.1:80-88
 - 指定端口的时候，只能使用 tcp 或 udp 协议，而 all 还包括 icmp 等协议（ping 使用 icmp）
- 可以建立多条规则，在规则冲突的情况下，以序号小的规则优先，序号 1 为最优规则

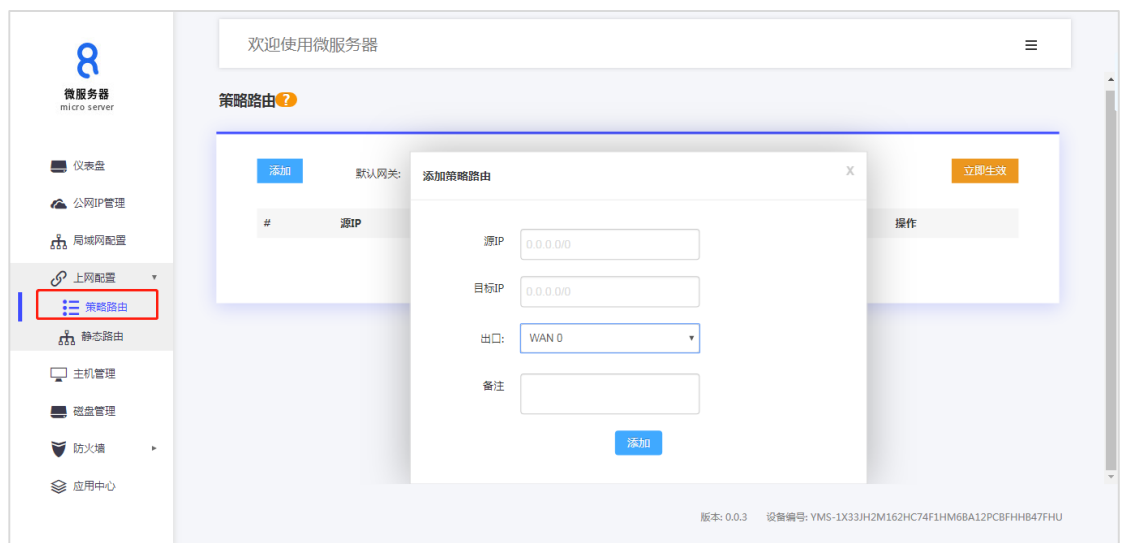
- 慎用禁止访问功能，尤其是目标为微服务器自身或所属 IP 段时，设置不当可能造成无法访问微服务器，如果一定要设置，至少先建立一条允许 LAN 访问微服务器的规则，且置顶

4. 路由策略设置

可以添加多 wan 出口策略和静态路由策略，在“上网配置”中设置

- 策略路由：

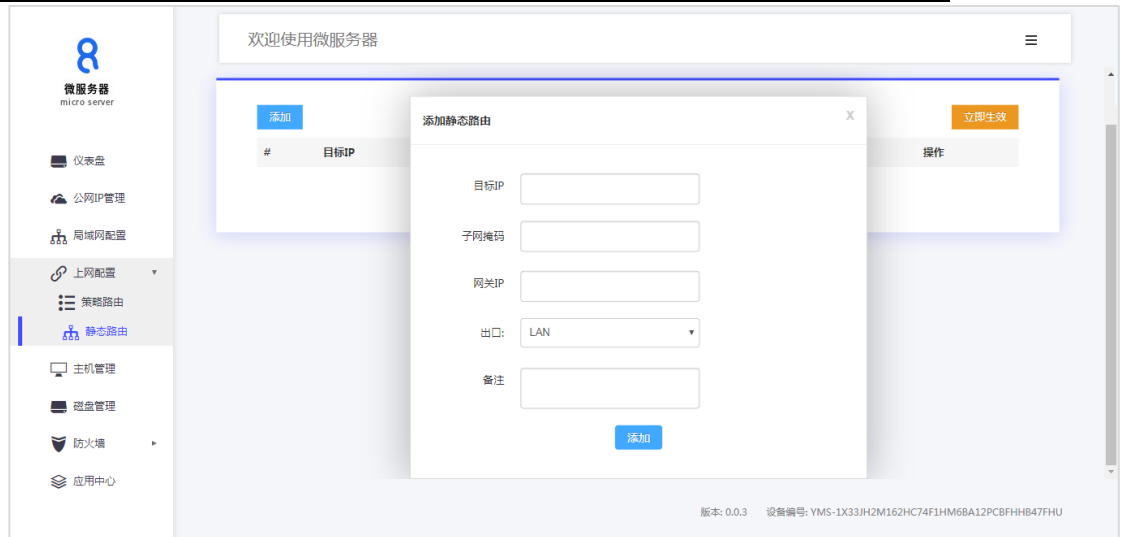
相当于多 wan 口路由器的上网策略，可以设置某些网段通过指定 wan 口出站



- 源 IP 和目的 IP，可以全填或选填其一，支持 IP 范围
- 有多 wan 口的情况下，可以设置某一个 wan 口为默认出口，然后再对另一个 wan 口增加策略，更方便

- 静态路由：

相当于操作系统的 route 命令，添加内网访问指定 IP（段）时使用的网关



- 如：指定访问 114.114.114.114，子网掩码为 255.255.255.255（只对 114 生效），网关 IP 为 192.168.1.1，出口为 wan，那么内网所有访问 114 的数据包都会从 192.168.1.1 传输
- 相对于策略路由，静态路由可以设置 lan-lan 的路由规则

5. 端口映射

这里的端口映射是在通过微服务器自身 wan 口的 IP 访问时生效，对微服务器的固定公网 IP 不生效

端口映射

名称:

协议:

源zone:

源目标端口:

更多配置

源IP:

源端口:

源目标IP:

NAT 回环:

转发目标zone:

转发目标IP:

转发目标端口:

- 名称: 任意填写
- 协议: 可选 TCP、UDP、TCP+UDP
- 源 zone: lan 或 wan, 传统端口映射描述的为 wan 到 lan 的映射
- 源目标端口: 即传统描述的外部端口, 如 80, 或 80—90
- 更多配置: 可以进一步指定源 IP、源端口和源目标 IP
- NAT 回环: 可选中, 支持最初的源和最终目的都在 NAT 内 (如两个不同 vlan)
- 转发目标 zone: lan 或 wan
- 转发目标: 即传统描述的内部 IP
- 转发目标端口: 即传统描述的内部端口, 可以指定范围, 如 80, 或 80—90

要达到传统路由的端口映射功能, 主要填写源目标端口 (外部端口)、转发目标 IP (内网 IP)、转发目标端口 (内部端口)