易维宝智能业务应用运维

管理平台用户使用手册

V6.0

目 录

1 安装部署

1.1 如何下载 DCS

使用浏览器（Chrome、Edge）打开“智能业务应用运维管理平台” portal.ewb81.com，依次进行如下操作：

1）点击进入“系统管理”页面

2）点击左侧页签，进入“DCS 信息”页面

3）点击右下方“下载 DCS 文件”按钮

4）下载自动开始，等待完成

1.2 如何安装 DCS

在采集服务器上，依次进行如下操作：

1）使用 root 账号登录服务器，确认可以访问 CCS 服务器地址，可以使用 ping 工具验证。

[root@server ~] ping ccs.ewb81.com

2）[root@server ~] cd [DCS 安装文件所在目录]

3）[root@server ~] unzip dcs.zip && chmod +x ./saas_dcs_installer.bin && ./saas_dcs_installer.bin

4）[root@server ~] 输入 CCS 连接端口、连接密钥后，多次下一步完成安装

5）[root@server ~] cd [DCS 安装目录]/its_run/dcs_run/bin && sh start.sh

6）登录到运维管理平台 portal.ewb81.com，发现资源

1 发现资源

每个资源的发现规则和设置都不一样，发现资源时可以参考资源模型下方的帮助提示，可以根据提示引导做发现前的设置。

1.1 主机

1.1.1 Linux 主机

使用系统发现 Linux 主机时，需要前置条件，发现前提满足后即可以被发现。

1.1.1.1 发现前提

1.1.1.1.1 需要安装 iostat、lsof、python2 命令

下面的例子以 CentOS 系统，其他 Linux 系统使用各自系统的命令

1) 检查是否已经安装 iostat 命令

```
[root@server ~]# iostat -V
```

2) 安装 iostat 命令方法

```
[root@server ~]# yum install lsof
```

3) 检查是否已经安装 lsof 命令

```
[root@server ~]# lsof -v
```

4) 安装 lsof 命令方法

```
[root@server ~]# yum install lsof
```

5) 检查是否已经安装 python2 命令

需要确认输入 python 命令，默认指向的是 python2，而并不是 python3

```
[root@server ~]# python -V
```

6) 检查是否已经安装 python2 命令

```
[root@server ~]# yum install python2
```

1.1.1.1.2需要将 SSH 服务 TCP 端口加入到系统防火墙规则

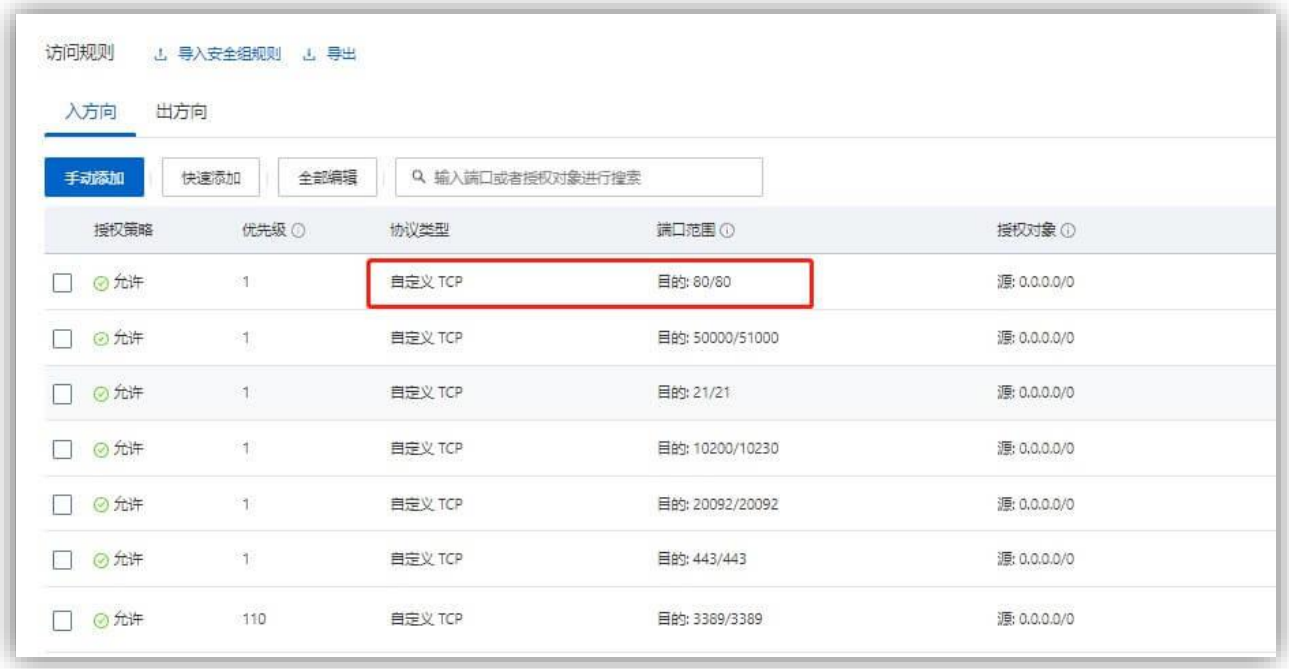
1) 检查 SSH 服务 TCP 端口是否加入到系统防火墙规则

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

2) SSH 服务 TCP 端口加入到系统防火墙规则方法

- 具体操作方法请参考如下链接：
  https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 SSH 端口



4) 如果为云服务器，检查是否已经打开 SSH 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明：
  https://help.aliyun.com/document_detail/25471.html

1.1.1.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单

图 2-1 资源管理页面

- 点击左侧资源列表，从弹出的窗口中点击“发现资源”按钮

图 2-2 资源列表页面

- 在资源模型下拉列表中依次点击选择主机、Linux 主机、Linux SSH 监控模型

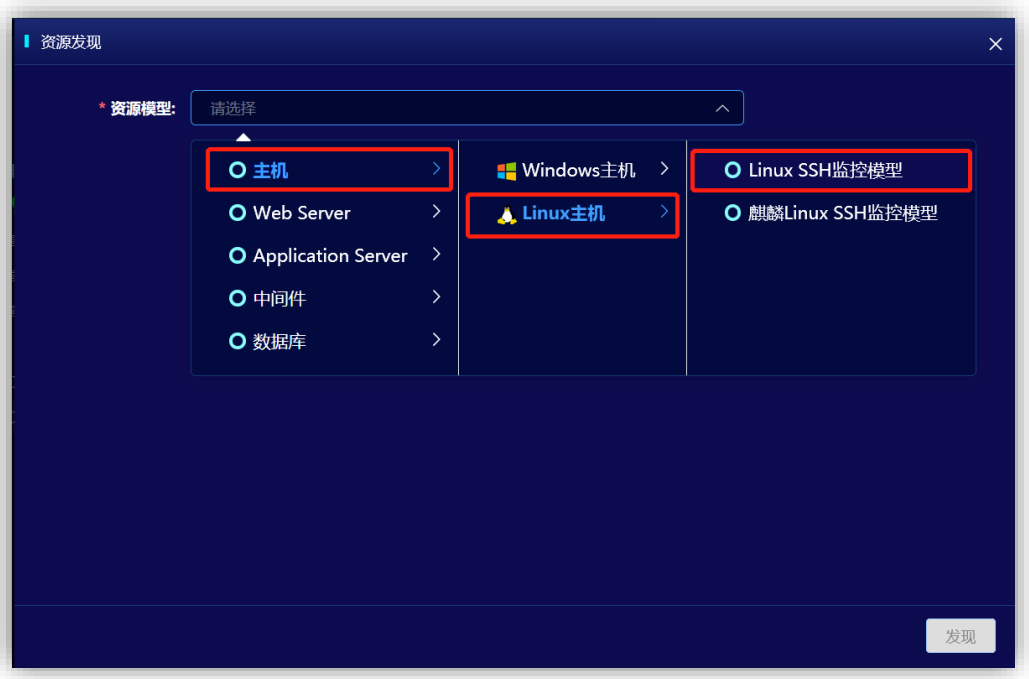


图 2-3 资源发现页面

- 从下面的窗口中输入 IP 地址、SSH 端口、用户名、密码后，点击“发现”按钮。

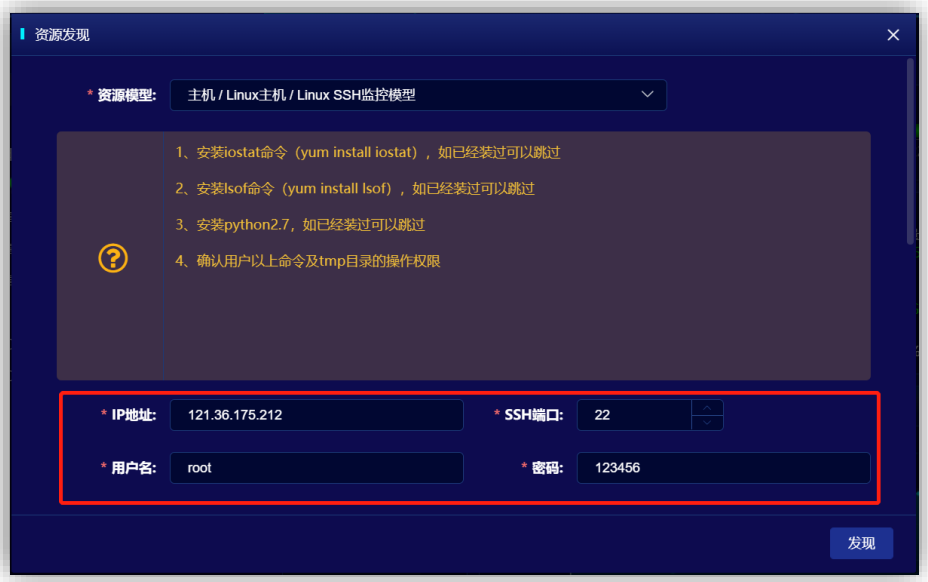


图 2-4 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源

图 2-5 发现资源后的资源列表

- 点击资源后，进入主机概览页

图 2-6 Linux 主机概览页

1.1.2 Windows 主机

使用系统发现 Windows 主机时，需要安装及开启 SNMP 服务，开启并配置完成后即可以被发现。

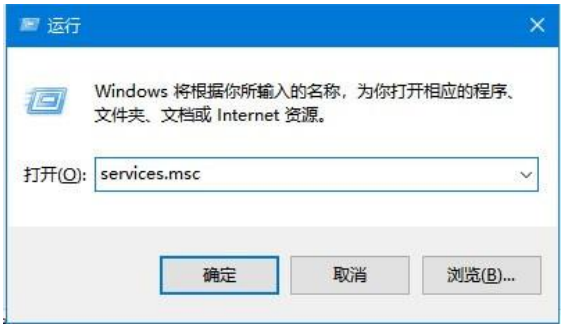
以下的操作适用于 Windows 2003 及以上的操作系统版本。以下以 Windows 2008 版本为例。

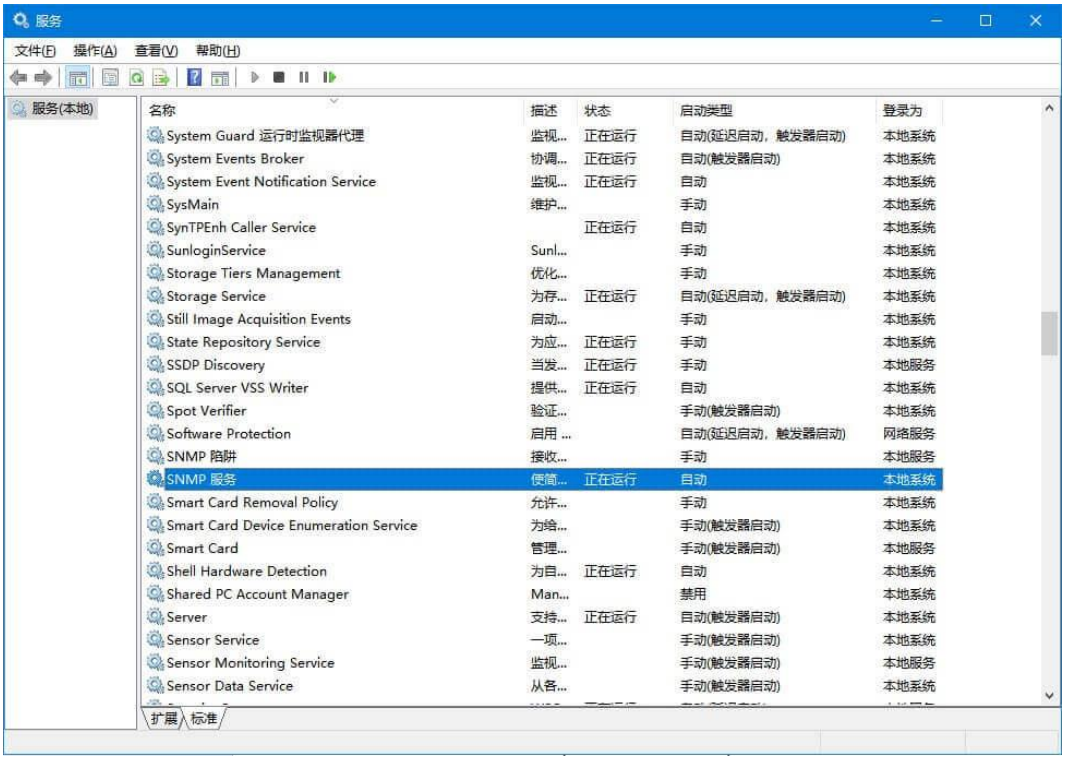
1.1.2.1 发现前提

1.1.2.1.1 需要安装 SNMP 服务并打开 SNMP 端口

1) 检查是否已经安装 SNMP 服务

在服务器管理器窗口中查看是否存在 SNMP Service 服务





2) 安装 SNMP 服务方法

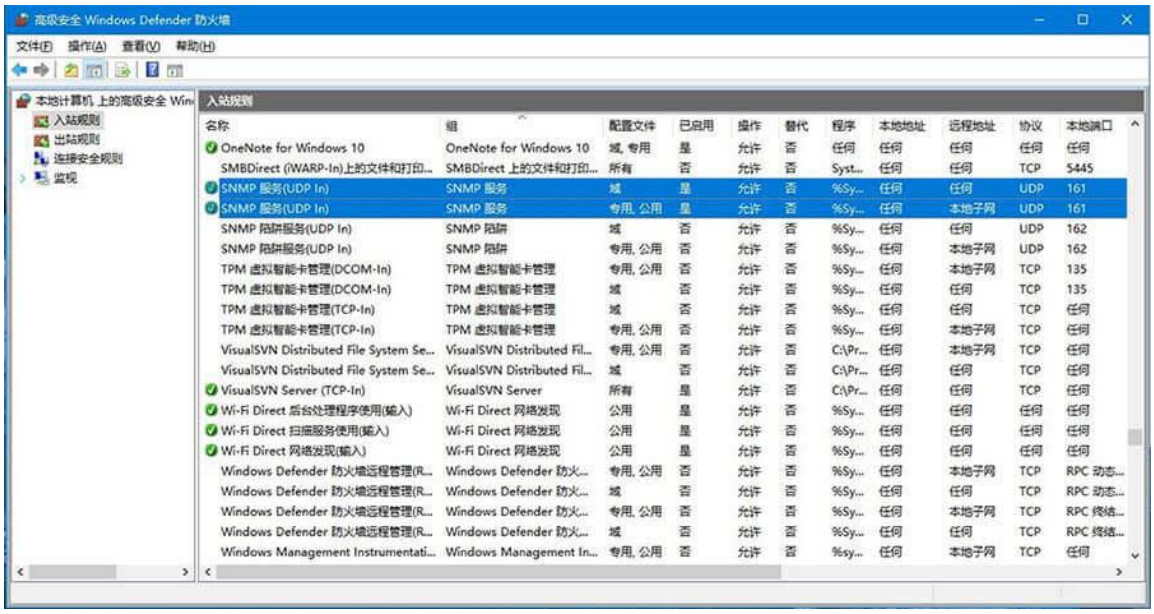
具体操作方法请参考如下链接：

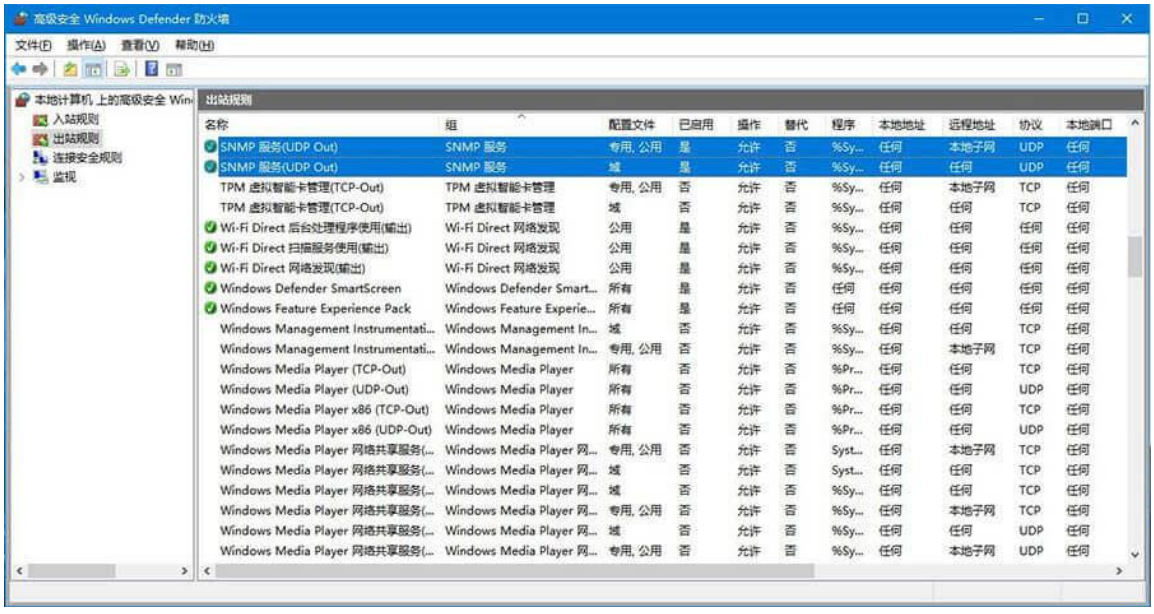
https://jingyan.baidu.com/article/4e5b3e193959ef91901e24bf.html

1.1.2.1.2 需要将 SNMP 服务 TCP 端口加入到系统防火墙规则

1) 检查 SNMP 服务 UDP 端口是否加入到系统防火墙规则

查看 Windows 防火墙中的入站和出站规则中是否存在 161 端口的 UDP 规则





2) SNMP 服务 UDP 端口加入到系统防火墙规则方法

- 具体操作方法请参考如下链接：

https://jingyan.baidu.com/article/77b8dc7f9ff91d6174eab6a3.html

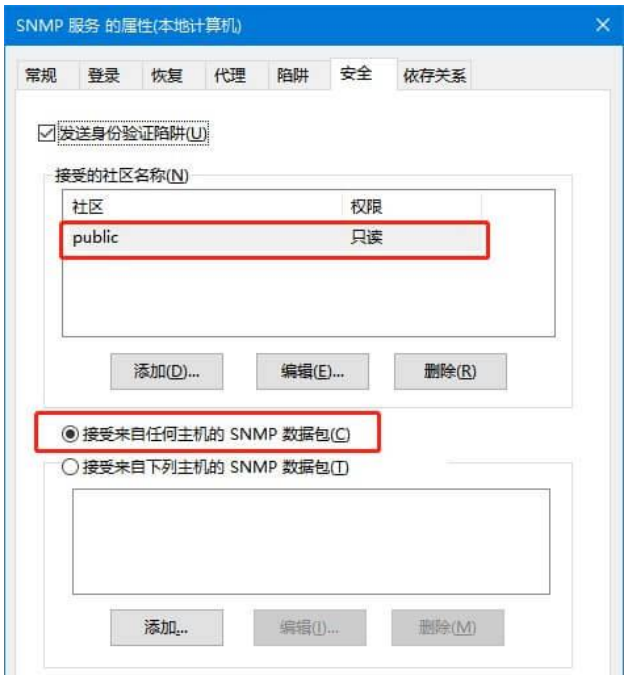
3) 如果为云服务器，检查是否已经打开 SSH 端口

4) 云服务器开启 SNMP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：
  https://help.aliyun.com/document_detail/25471.html

1.1.2.1.3 需要允许远程访问 SNMP 服务

1) 检查是否允许远程访问 SNMP 服务



2) 打开允许远程访问 SNMP 服务方法

- 具体操作方法请参考如下链接：

https://www.cnblogs.com/personsiglewine/p/11609148.html

1.1.2.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 Windows SNMP 监控模型

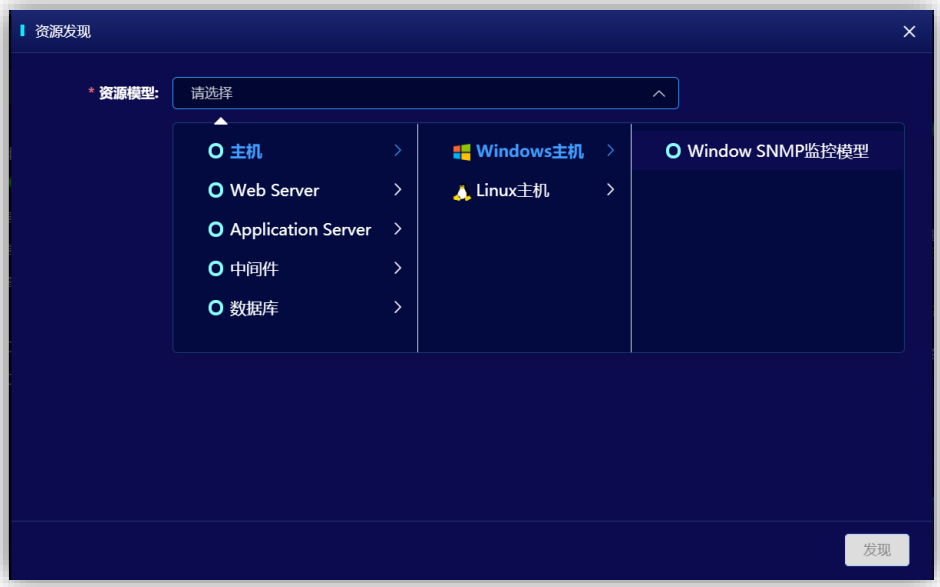


图 2-7 资源发现页面

- 从下面的窗口中输入 IP 地址、端口、只读共同体、读写共同体后，点击“发现”按钮。

图 2-8 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源

图 2-9 发现资源后的资源列表

- 点击资源后，进入主机概览页

图 2-10 Windows 主机概览页

1.2 Web Server

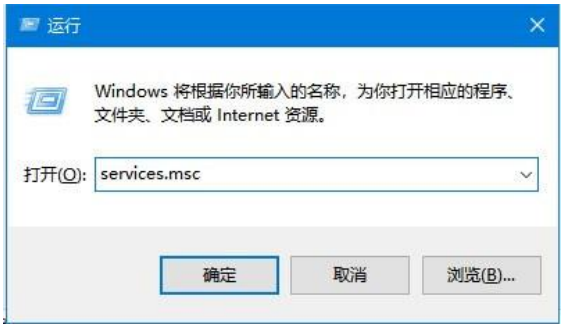
1.2.1 IIS

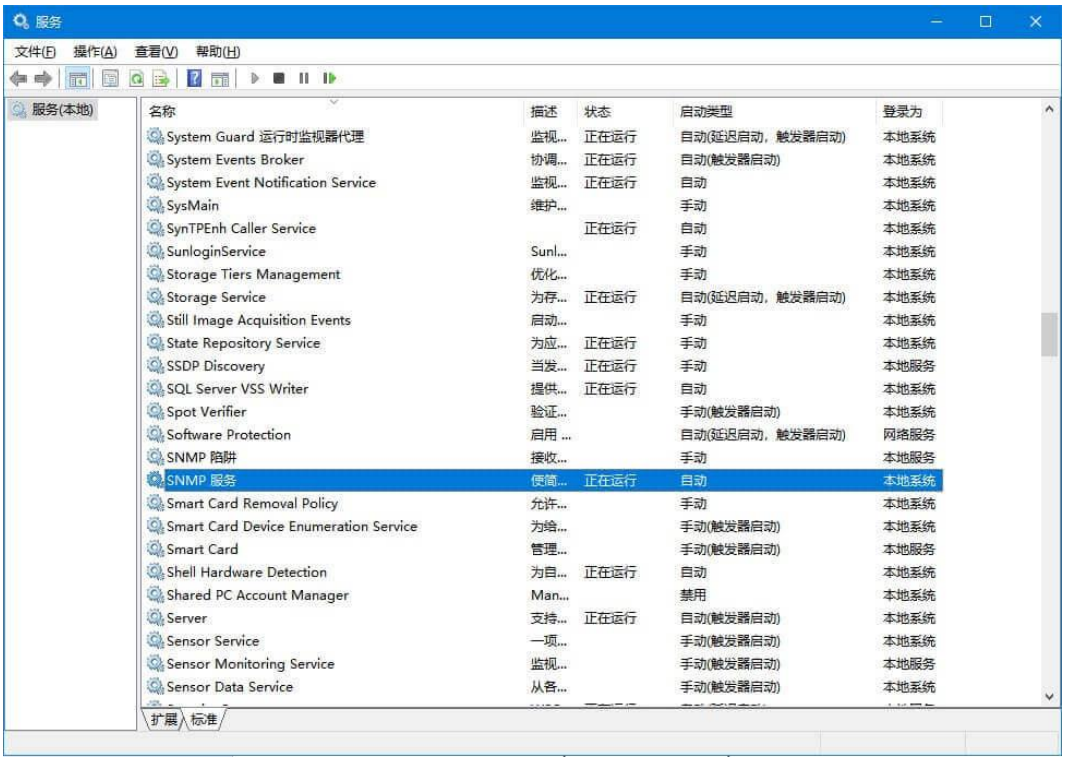
1.2.1.1 发现前提

1.2.1.1.1 需要安装 SNMP 服务并打开 SNMP 端口

1) 检查是否已经安装 SNMP 服务

在服务器管理器窗口中查看是否存在 SNMP Service 服务





2) 安装 SNMP 服务方法

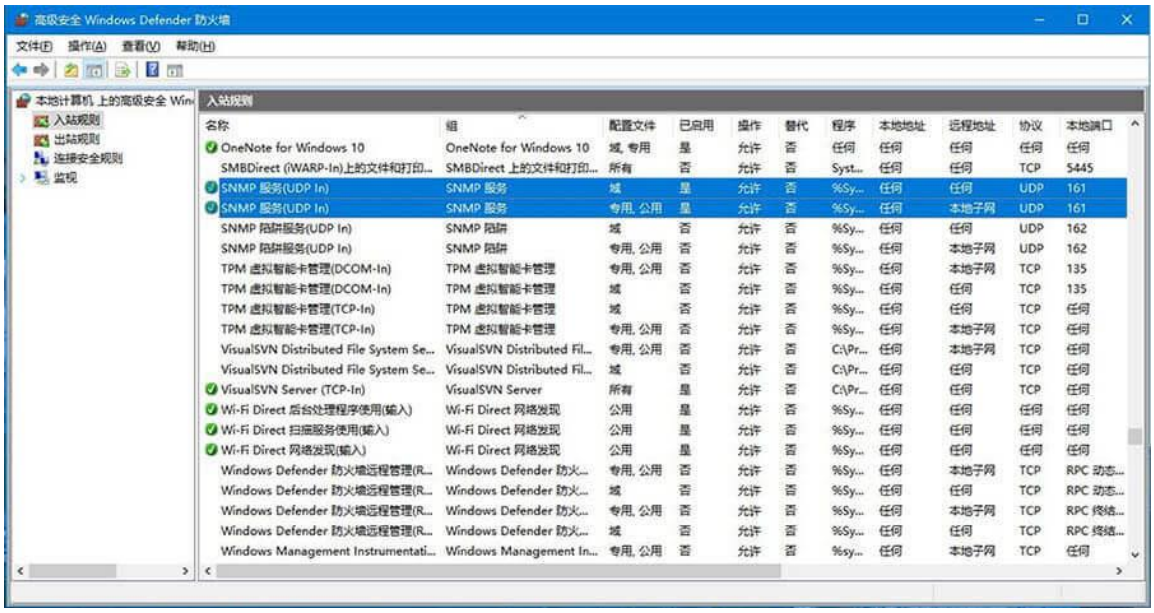
具体操作方法请参考如下链接：

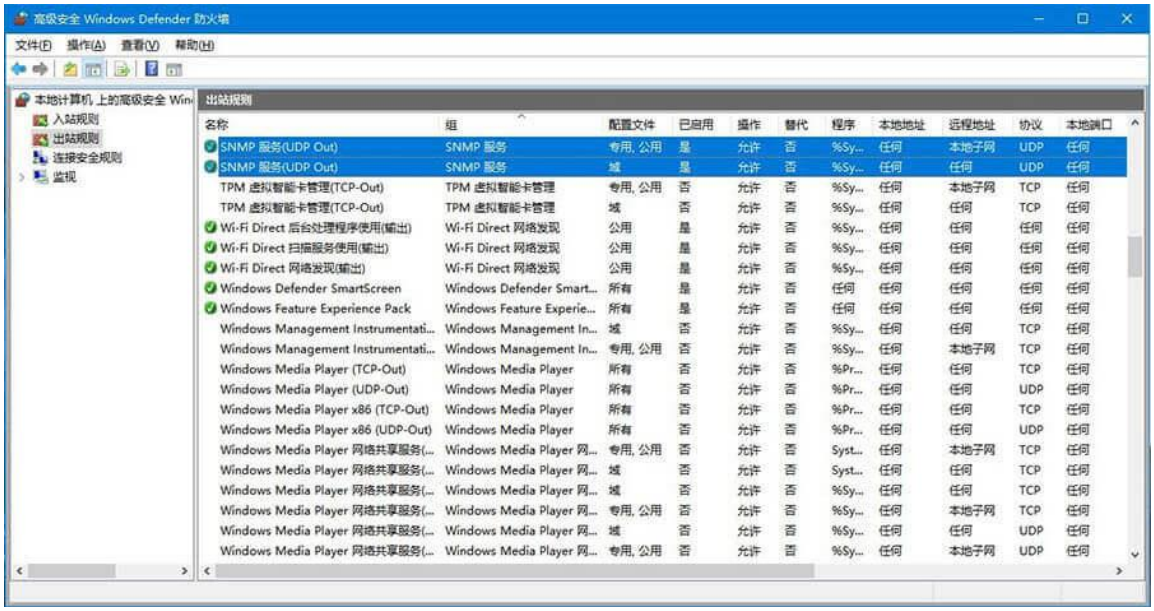
https://jingyan.baidu.com/article/4e5b3e193959ef91901e24bf.html

1.2.1.1.2 需要将 SNMP 服务 TCP 端口加入到系统防火墙规则

1) 检查 SNMP 服务 UDP 端口是否加入到系统防火墙规则

查看 Windows 防火墙中的入站和出站规则中是否存在 161 端口的 UDP 规则





2) SNMP 服务 UDP 端口加入到系统防火墙规则方法

- 具体操作方法请参考如下链接：

https://jingyan.baidu.com/article/77b8dc7f9ff91d6174eab6a3.html

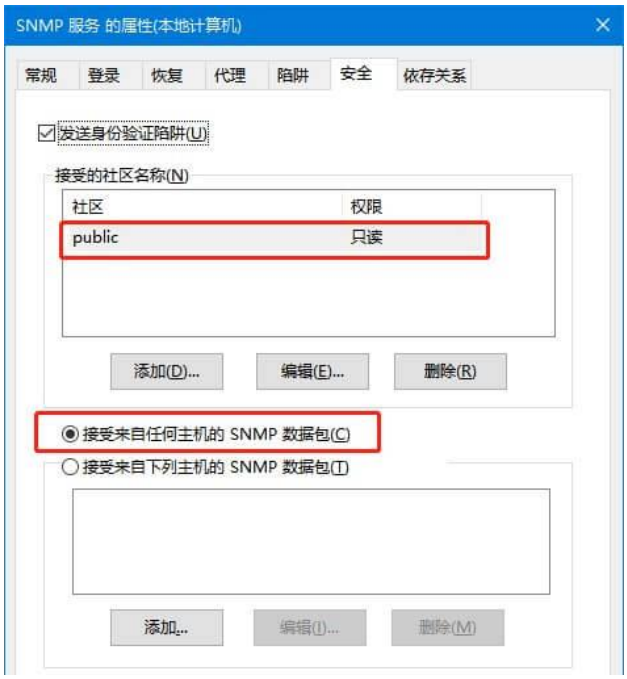
3) 如果为云服务器，检查是否已经打开 SSH 端口

4) 云服务器开启 SNMP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：
  https://help.aliyun.com/document_detail/25471.html

1.2.1.1.3 需要允许远程访问 SNMP 服务

1) 检查是否允许远程访问 SNMP 服务



2) 打开允许远程访问 SNMP 服务方法

- 具体操作方法请参考如下链接：

https://www.cnblogs.com/personsiglewine/p/11609148.html

1.2.1.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 IIS V6.0 及以上版本

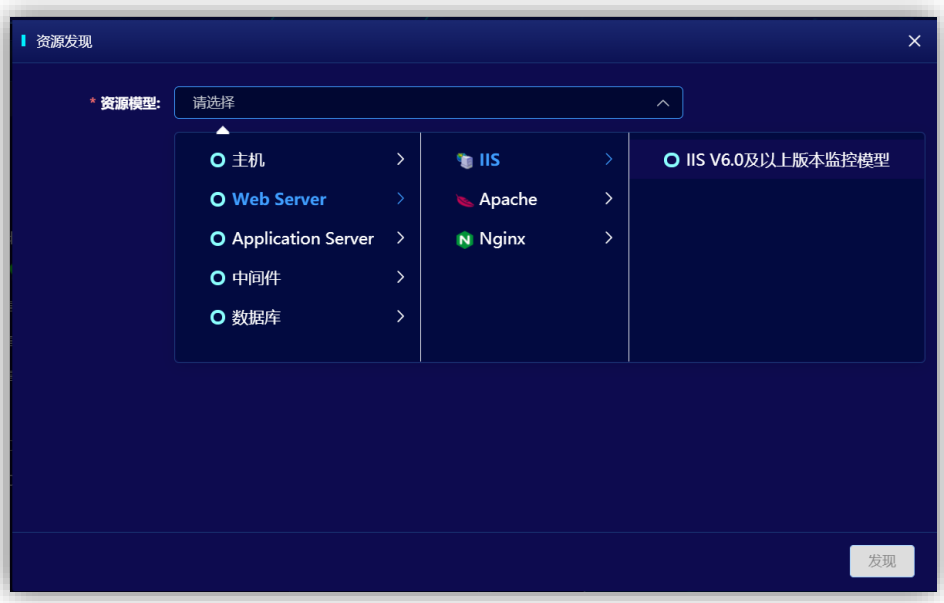


图 2-11 资源发现页面

- 从下面的窗口中输入 IP 地址、端口、只读共同体，读写共同体。

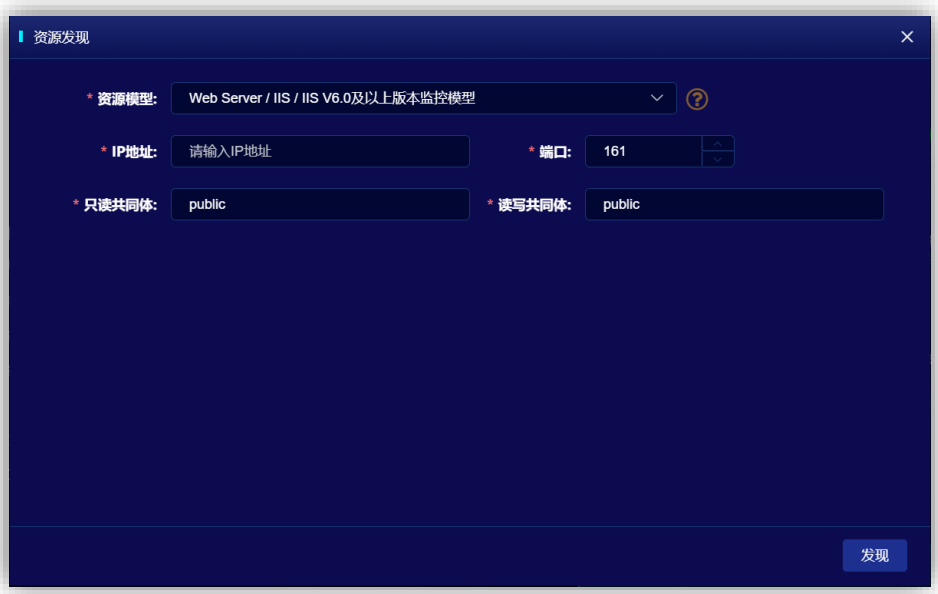


图 2-12 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-13 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-14 资源概览页

1.2.2 Apache

1.2.2.1 发现前提

1.2.2.1.1 如果 Apache 所在主机未被发现，请先检查主机是否满足发现前提

windows 或 linux

1.2.2.1.2 需要开启自定义格式的 access_log、开启 status_module.so 模块、开启 server-status/server-info 请求块

以下的操作步骤及配置方法是在 Linux 环境下，Windows 环境下的配置方法相同。

1) 检查是否开启自定义格式的 access_log

- 确认 httpd.conf 配置文件是否开启自定义 access_log

```
[root@server ~]# cat /etc/httpd/conf/httpd.conf | grep monitor

LogFormat        '{"ip":"%a","time":"%{ms}T","path":"%r","status":"%>s","bytes":"%b"}'
```

```
monitor

CustomLog 'logs/monitor_access.log' monitor
```

2) 自定义格式的 access_log 开启方法

- httpd.conf 配置文件开启自定义 access_log 方法

```
<IfModule log_config_module>

......

LogFormat       "{"ip":"%a","time":"%{ms}T","path":"%r","status":"%>s","bytes":"%b"}"

monitor

......

CustomLog "logs/monitor_access.log" monitor

</IfModule>
```

3) 检查 mod_status.so 模块是否开启

- 确认 httpd.conf 配置文件中是否开启 httpd-info.conf 和 conf.d/*.conf

```
[root@server ~]# cat /etc/httpd/conf/httpd.conf | grep httpd-info.conf

# Mutex directive, if file-based mutexes are used. If you wish to share the

Include /usr/share/doc/httpd/httpd-info.conf



[root@server ~]# cat /etc/httpd/conf/httpd.conf | grep conf.d

# Load config files in the '/etc/httpd/conf.d' directory, if any.

IncludeOptional conf.d/*.conf
```

- 确认 00-base.conf 配置文件是否开启 mod_status.so

```
[root@server ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep mod_status.so

LoadModule status_module modules/mod_status.so
```

4) mod_status.so 模块开启方法

- httpd.conf 配置文件开启 httpd-info.conf 和 conf.d/*.conf 方法

```
编辑 /etc/httpd/conf/httpd.conf 配置文件

去掉 #Include /usr/share/doc/httpd/httpd-info.conf 前面的#号

去掉 #IncludeOptional conf.d/*.conf 前面的#号
```

- 00-base.conf 配置文件开启 mod_status.so 方法

```
LoadModule status_module modules/mod_status.so

去掉 #LoadModule status_module modules/mod_status.so 前面的#号
```

5) 检查是否开启 server-status/server-info 请求块

```
[root@server ~]# cat /usr/share/doc/httpd/httpd-info.conf | grep server-status

# mod_status (for the server-status handler)

# with the URL of http://servername/server-status

<Location /server-status>

SetHandler server-status

# Off) when the 'server-status' handler is called. The default is Off.

[root@server ~]# cat /usr/share/doc/httpd/httpd-info.conf | grep server-info

# mod_info (for the server-info handler),

# http://servername/server-info (requires that mod_info.c be loaded).

<Location /server-info>
```

```
SetHandler server-info
```

6) 开启 server-status/server-info 请求块开启方法

- 在/usr/share/doc/httpd/httpd-info.conf 中增加 /server-status 请求路径

```
<Location /server-status>

SetHandler server-status

</Location>
```

- 在/usr/share/doc/httpd/httpd-info.conf 中增加 /server-info 请求路径

```
<Location /server-info>

SetHandler server-info

</Location>
```

1.2.2.1.3 需要在配置文件修改后重新启动 httpd 服务

```
[root@server ~]# systemctl restart httpd
```

1.2.2.1.4 需要将 httpd 服务 TCP 端口加入到系统防火墙规则

1) 检查 httpd 服务 TCP 端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) httpd 服务 TCP 端口加入到系统防火墙规则方法

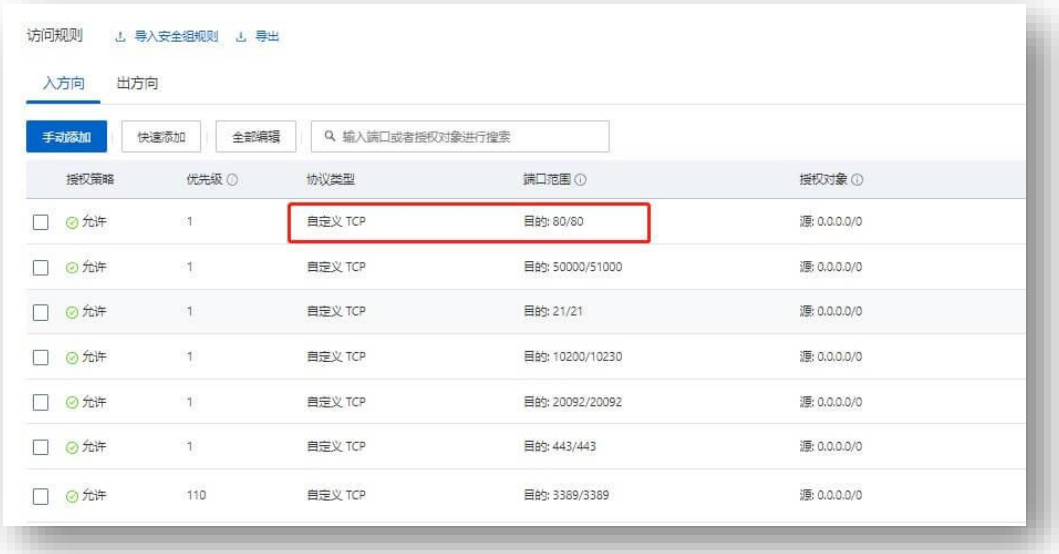
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 httpd 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:80/80（或者自定义端口号）。



4) 云服务器开启 httpd 服务端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.2.2.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 Apache V2.x 及以上版本

图 2-15 资源发现页面

- 从下面的窗口中输入 IP 地址、端口、选择主机模型后输入对应的连接信息。

图 2-16 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-17 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-18 资源概览页

1.2.3 Nginx

1.2.3.1 发现前提

1.2.3.1.1 如果 Nginx 所在主机未被发现，请先检查主机是否满足发现前提

1.2.3.1.2 需要开启自定义格式的 access_log、开启 http_stub_status_module 模块、开启 location 块级指令 ngx_status

1) 检查是否开启自定义格式的 access_log

在 /usr/local/nginx/conf/nginx.conf 或 /etc/nginx/nginx.conf 配置文件中是否有 access_log ..... monitor 的定义

2) 开启自定义格式的 access_log 方法

- 在 nginx.conf 配置文件的 http 段中新增 access_log 定义

```
http {

include mime.types;

default_type application/octet-stream;

log_format monitor '{"ip":"$remote_addr","time":

ime","path":"$request","status":"$status","bytes":"$bytes_sent"}';access_log

/tmp/logs/monitor_access.log monitor;

.....

}
```

3) 需要开启 http_stub_status_module 模块

- 检查是否开启 http_stub_status_module 模块

```
[root@server ~]# nginx -V

nginx version: nginx/1.16.1

built by gcc 4.8.5 20150623 (Red Hat 4.8.5-39) (GCC)

TLS SNI support enabled

configure arguments: --prefix=/usr/share/nginx --sbin-path=/usr/sbin/nginx --modules-

path=/usr/lib64/nginx/modules --conf-path=/etc/nginx/nginx.conf --error-log-

path=/var/log/nginx/error.log --http-log-path=/var/log/nginx/access.log --with-

http_stub_status_module
```

- 开启 http_stub_status_module 模块方法

  具体操作方法参见如下链接地址：
  https://blog.csdn.net/memory6364/article/details/84326896

4) 需要开启 location 块级指令 ngx_status

- 检查是否开启 location 块级指令

确认 nginx.conf 或自定义 conf 配置文件中的 server 段是否包含配置

```
location /ngx_status {
    stub_status on;
}
```

- 开启 location 块级指令方法

在 nginx.conf 或自定义 conf 配置文件中新增 server 段配置，也可以在已有的 server 段增加如下配置

```
location /ngx_status {
    stub_status on;
}
```

- 重新加载 nginx 配置文件，使配置生效

```
[root@server ~]# nginx -s reload
```

1.2.3.1.3 需要将 nginx 监听的 TCP 端口加入到系统防火墙规则

1) 检查 nginx 监听的 TCP 端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) nginx 监听的 TCP 端口加入到系统防火墙规则方法

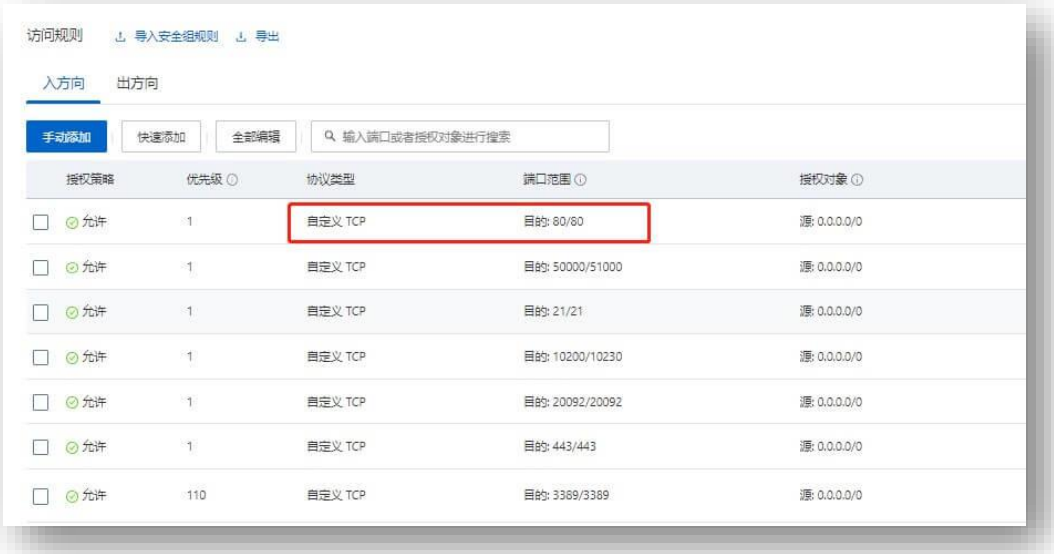
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 nginx 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:80/80（或者自定义端口号）。



4) 云服务器开启 nginx 服务端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.2.3.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 Nginx V1.16 及以上版本

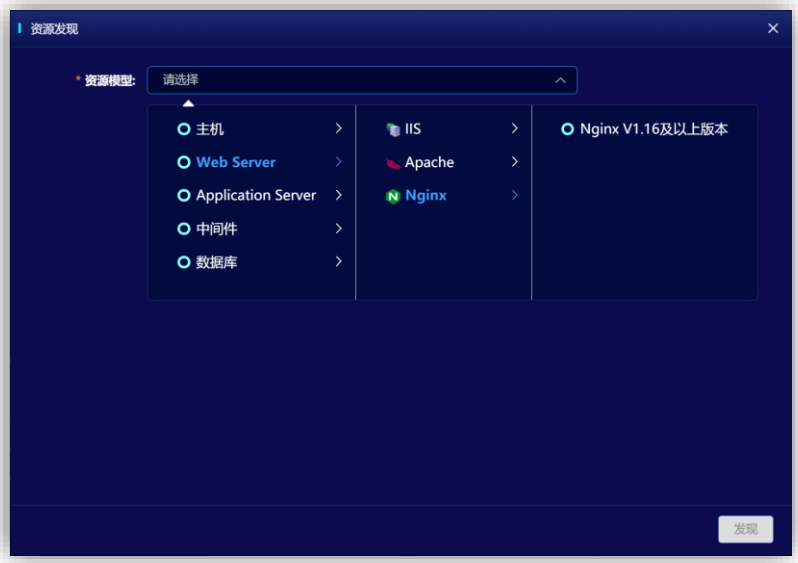


图 2-19 资源发现页面

- 从下面的窗口中输入 IP 地址、端口、输入 Linux 主机信息确定。

图 2-20 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-21 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-22 资源概览页

1.3 Application Server

1.3.1 Jetty

1.3.1.1 发现前提

需要确定被监控的 JETTY 的 JAVA 应用的开发部署模式属于嵌入式（Springboot 模式还是非嵌入模式)。

- 嵌入模式：应用与 Jetty 容器一同被打包发布，典型的模式为 SpringBoot。
- 非嵌入模式：应用与 Jetty 容器分离，典型的模式为使用 Jetty 容器。

1.3.1.1.1 如果 Jetty 所在主机未被发现，请先检查主机是否满足发现前提

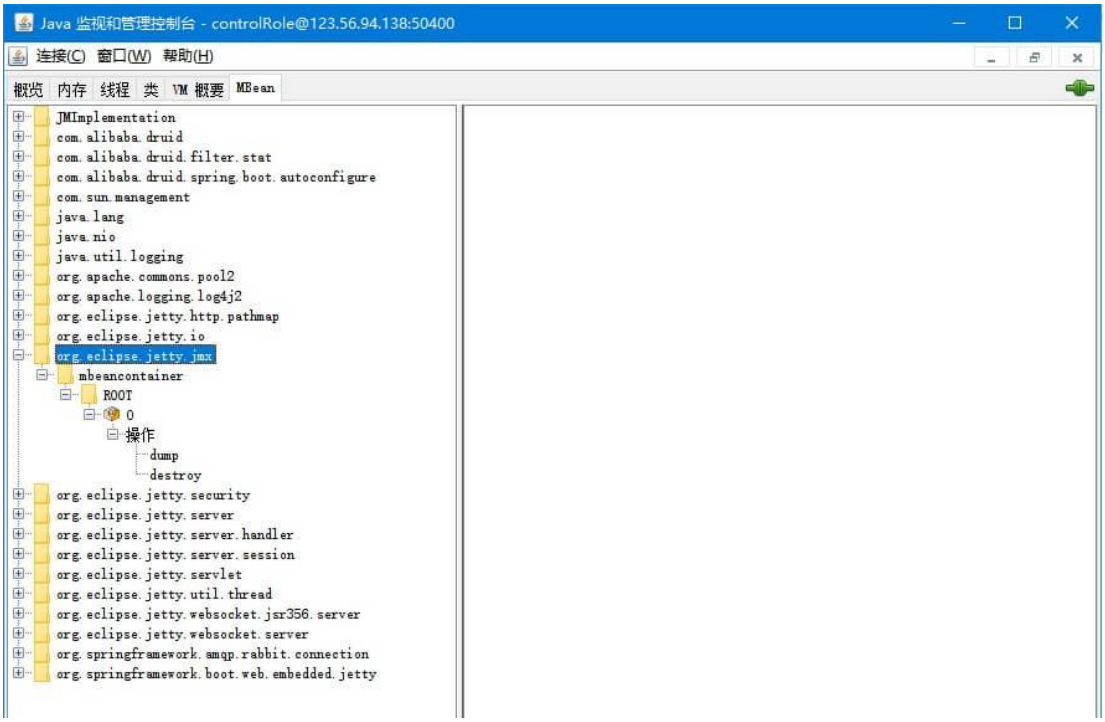
windows 或 linux

1.3.1.1.2 使用嵌入式（Springboot）方式打包并发布项目

以下的操作步骤及配置方法是在 Linux 环境下，Windows 环境下的配置方法相同。

1) 需要开启 JAVA 应用的 JMX 远程访问

- 使用 jconsole.exe 远程连接被监控端的 JMX 端口



2) 开启 JAVA 应用的 JMX 远程访问方法

- 下载 JAR 包并确认激活 JMX 远程访问

可通过百度下载应用使用的 jetty 版本对应的 JMX 包，应为 jetty-jmx-*.jar 包，从监控系统的 DCS 安装包中或 Server 包中提取 its-client-plugin-monitor-*.jar 包复制到 jetty 应用的 classpath 中，并使 JAVA 应用启动时可以加载到这两个 JAR 包。

- 开启 JMX 远程访问的用户密码权限配置

如果需要使用用户名密码的 JMX 远程访问方式时，可以通过下面的方式建立访问权限控制文件，并放置到/home/jmxremote 目录下。

权限控制文件 jmxremote.access 内容如下：

```
controlRole readwrite

create javax.management.monitor.*,javax.management.timer.*

unregister
```

权限控制文件 jmxremote.password 内容如下：

```
controlRole R&D
```

设置权限控制文件为只读模式：

```
[root@server ~]# chmod 400 jmxremote.access

[root@server ~]# chmod 400 jmxremote.password
```

- 需要在 JAVA 应用的启动命令上增加 JMXREMOTE 参数

  检查 JAVA 应用的启动命令是否开启 JMXREMOTE 参数

```
... ... -Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=1100 -
Dcom.sun.management.jmxremote.rmi.port=1100 -Dcom.sun.management.jmxremote.ssl=false -
Dcom.sun.management.jmxremote.authenticate=false
```

  配置 JAVA 应用的启动命令开启 JMXREMOTE 参数方法

```
-Dcom.sun.management.jmxremote

-Dcom.sun.management.jmxremote.port=8163

-Dcom.sun.management.jmxremote.rmi.port=8163

-Dcom.sun.management.jmxremote.ssl=false

-Djava.rmi.server.hostname=10.36.175.212 //IP 地址需要与外网访问地址一致

// 下面参数为使用用户名密码的方式启用远程访问时的参数，不启用可以不增加

-Dcom.sun.management.jmxremote.authenticate=true

-Dcom.sun.management.jmxremote.access.file=/home/jmxremote/jmxremote.access

-Dcom.sun.management.jmxremote.password.file=/home/jmxremote/jmxremote.password
```

1.3.1.1.3 使用非嵌入式（自定义启动脚本）方式打包并发布项目

以下的操作步骤及配置方法是在 Linux 环境下，Windows 环境下的配置方法相同。

1) 需要在启动脚本中增加 JMXREMOTE 配置、JETTY 容器开启 JETTY-JMX 模块、自定义启动脚本增加 JMXREMOTE 配置

- 检查启动脚本 JMXREMOTE 配置

  检查 bin/jetty.sh 的 JAVA_OPTIONS 变量是否包含下面配置。

```
"-Dcom.sun.management.jmxremote"

"-Dcom.sun.management.jmxremote.port=8162"

"-Dcom.sun.management.jmxremote.rmi.port=8162"

"-Dcom.sun.management.jmxremote.ssl=false"

"-Djava.rmi.server.hostname=121.36.175.1"
```

- 启动脚本增加 JMXREMOTE 配置方法

  bin/jetty.sh 的 JAVA_OPTIONS 变量按照下面的参数进行配置。

```
JAVA_OPTIONS=(${JAVA_OPTIONS[*]}

"-Djetty.home=$JETTY_HOME"

"-Djetty.base=$JETTY_BASE"

"-Djava.io.tmpdir=$TMPDIR"

"-Dcom.sun.management.jmxremote"

"-Dcom.sun.management.jmxremote.port=8162"

"-Dcom.sun.management.jmxremote.rmi.port=8162"

"-Dcom.sun.management.jmxremote.ssl=false"

"-Djava.rmi.server.hostname=121.36.175.1"

"-Dcom.sun.management.jmxremote.authenticate=true"

"-Dcom.sun.management.jmxremote.access.file=/home/jmxremote/jmxremote.access"
```

```
"-Dcom.sun.management.jmxremote.password.file=/home/jmxremote/jmxremote.password"

)
```

- 开启 JMX 远程访问的用户密码权限配置

如果需要使用用户名密码的 JMX 远程访问方式时，可以通过下面的方式建立访问权限控制文件，并放置到/home/jmxremote 目录下。

```
// 权限控制文件 jmxremote.access 内容

controlRole readwrite

create javax.management.monitor.*,javax.management.timer.*

unregister

// 权限控制文件 jmxremote.password 内容

controlRole R&D
```

设置权限控制文件为只读模式：

```
[root@server ~]# chmod 400 jmxremote.access

[root@server ~]# chmod 400 jmxremote.password
```

- 检查 JETTY 容器是否开启 JETTY-JMX 模块配置

确认 jetty/modules/server.mod 文件内容中开启 lib/jetty-jmx-${jetty.version}.jar 模块

确认 jetty/start.ini 文件内容中是否开启 server 模块

- JETTY 容器是否开启 JETTY-JMX 模块配置方法

修改 jetty/modules/server.mod 文件内容为下面配置方法

```
[lib]

.....
```

```
lib/jetty-jmx-${jetty.version}.jar

[xml]

......

etc/jetty-jmx.xml
```

修改 jetty/start.ini 文件内容，开启 server 模块配置

```
--module=server
```

- 检查自定义启动脚本 JMXREMOTE 配置

如果不使用 jetty 自带的启动脚本，而使用自定义启动脚本启动 Jetty 时，需要检查自定义启动脚本 start.sh 中是否包含下面配置。

```
# JMX CONFIG

JMX="-Dcom.sun.management.jmxremote"

JMX="$JMX -Dcom.sun.management.jmxremote.port=8162"

JMX="$JMX -Dcom.sun.management.jmxremote.rmi.port=8162"

JMX="$JMX -Dcom.sun.management.jmxremote.ssl=false"

JMX="$JMX -Djava.rmi.server.hostname=121.36.175.212"

JMX="$JMX -Dcom.sun.management.jmxremote.authenticate=true"

JMX="$JMX -Dcom.sun.management.jmxremote.access.file=/home/jmxremote/jmxremote.access

"

JMX="$JMX                                                                    -

Dcom.sun.management.jmxremote.password.file=/home/jmxremote/jmxremote.password"
```

- 自定义启动脚本 JMXREMOTE 配置方法

自定义启动脚本 start.sh 片段如下

```
JAVA_OPS="……$JMX"

nohup java $JAVA_OPS -jar -Dfile.encoding=UTF-8 start.jar --module=http >/dev/null 2>&1 &
```

1.3.1.1.4需要将 Jetty 的 JMX 监听的 TCP 端口加入到系统防火墙规则

1) 检查 JMX 监听的 TCP 端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) JMX 监听的 TCP 端口加入到系统防火墙规则方法

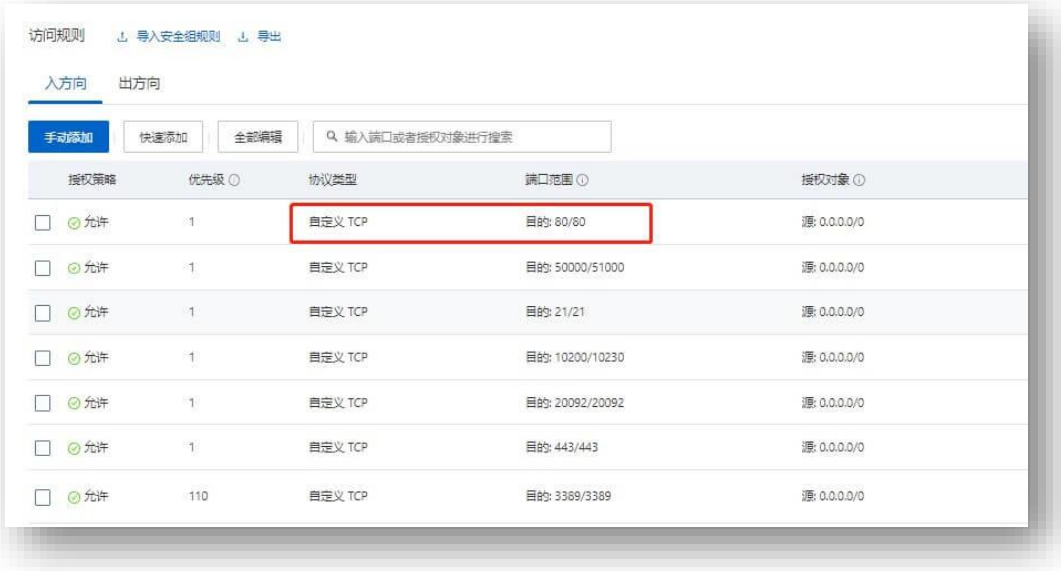
- 具体操作方法请参考如下链接:

Windows：https://blog.csdn.net/mineskey/article/details/110929469

Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 JMX 监听端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:8162/8162（或自定义端口号）



4) 云服务器开启 JMX 监听端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明:

  https://help.aliyun.com/document_detail/25471.html

1.3.1.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 Jetty V9.x 及以上版本

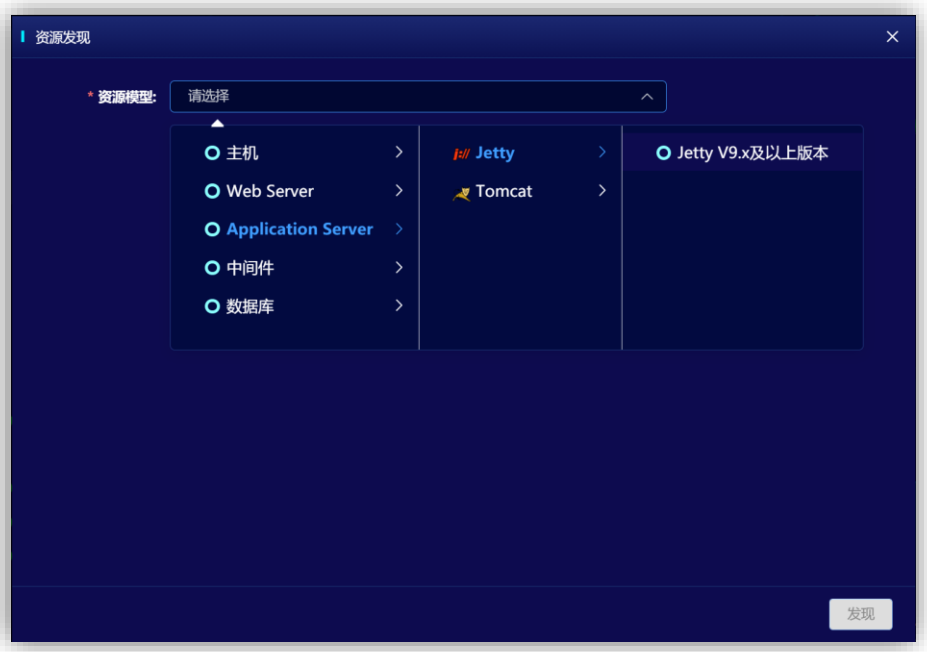


图 2-23 资源发现页面

- 从下面的窗口中输入 IP 地址、端口，用户名（对应 jmx 中权限模式的用户名）和密码（对应 jmx 中权限模式的密码），选择主机模型后输入对应的连接信息。

图 2-24 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-25 发现资源后的资源列表

图 2-26 资源概览页

1.3.2 Tomcat

1.3.2.1 发现前提

需要确定被监控的 Tomcat 的 JAVA 应用的开发部署模式属于嵌入式（Springboot 模式

还是非嵌入模式)。

- 嵌入模式：应用与 Tomcat 容器一同被打包发布，典型的模式为 SpringBoot。
- 非嵌入模式：应用与 Tomcat 容器分离，典型的模式为使用 Jetty 容器。

1.3.2.1.1 如果 Tomcat 所在主机未被发现，请先检查主机是否满足发现前提

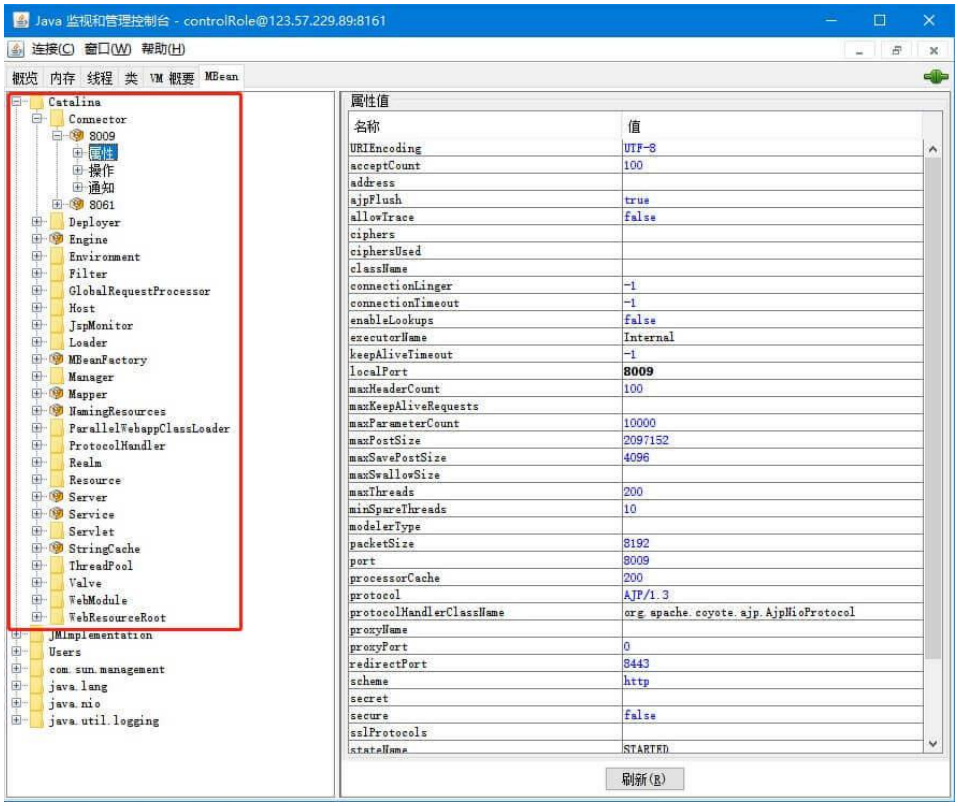
windows 或 linux

1.3.2.1.2 使用嵌入式（Springboot）方式打包并发布项目

以下的操作步骤及配置方法是在 Linux 环境下，Windows 环境下的配置方法相同。

1) 需要开启 JAVA 应用的 JMX 远程访问

- 使用 jconsole.exe 远程连接被监控端的 JMX 端口



2) 开启 JAVA 应用的 JMX 远程访问方法

- 开启 JMX 远程访问的用户密码权限配置

如果需要使用用户名密码的 JMX 远程访问方式时，可以通过下面的方式建立访问权限控制文件，并放置到/home/jmxremote 目录下。

权限控制文件 jmxremote.access 内容如下：

```
controlRole readwrite

create javax.management.monitor.*,javax.management.timer.*

unregister
```

权限控制文件 jmxremote.password 内容如下：

```
controlRole R&D
```

设置权限控制文件为只读模式：

```
[root@server ~]# chmod 400 jmxremote.access

[root@server ~]# chmod 400 jmxremote.password
```

- 需要在 JAVA 应用的启动命令上增加 JMXREMOTE 参数

  检查 JAVA 应用的启动命令是否开启 JMXREMOTE 参数

```
[root@server ~]# ps -ef | grep tomcat

-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=8161 -
Dcom.sun.management.jmxremote.rmi.port=8161 -Dcom.sun.management.jmxremote.ssl=false -
Dcom.sun.management.jmxremote.authenticate=true -Djava.rmi.server.hostname=123.57.229.89 -
Dcom.sun.management.jmxremote.access.file=/home/jmxremote/jmxremote.access -
Dcom.sun.management.jmxremote.password.file=/home/jmxremote/jmxremote.password
```

  配置 JAVA 应用的启动命令开启 JMXREMOTE 参数方法

```
-Dcom.sun.management.jmxremote
```

```
-Dcom.sun.management.jmxremote.port=8163

-Dcom.sun.management.jmxremote.rmi.port=8163

-Dcom.sun.management.jmxremote.ssl=false

-Djava.rmi.server.hostname=121.36.175.1 //IP 地址需要与外网访问地址一致

// 下面参数为使用用户名密码的方式启用远程访问时的参数，不启用可以不增加

-Dcom.sun.management.jmxremote.authenticate=true

-Dcom.sun.management.jmxremote.access.file=/home/jmxremote/jmxremote.access

-Dcom.sun.management.jmxremote.password.file=/home/jmxremote/jmxremote.password
```

1.3.2.1.3 使用非嵌入式（自定义启动脚本）方式打包并发布项目

以下的操作步骤及配置方法是在 Linux 环境下，Windows 环境下的配置方法相同。

1) 需要在启动脚本中增加 JMXREMOTE 配置

- 检查启动脚本 JMXREMOTE 配置

  检查 bin/catalina.sh 的 CATALINA_OPTIONS 变量是否包含下面配置。

```
"-Dcom.sun.management.jmxremote"

"-Dcom.sun.management.jmxremote.port=8161"

"-Dcom.sun.management.jmxremote.rmi.port=8161"

"-Dcom.sun.management.jmxremote.ssl=false"

"-Djava.rmi.server.hostname=121.36.175.1"
```

- 启动脚本增加 JMXREMOTE 配置方法

  bin/catalina.sh 的 CATALINA_OPTIONS 变量按照下面的参数进行配置。

```
CATALINA_OPTS="$CATALINA_OPTS
```

```
-Dcom.sun.management.jmxremote

-Dcom.sun.management.jmxremote.port=8161

-Dcom.sun.management.jmxremote.rmi.port=8161

-Dcom.sun.management.jmxremote.ssl=false

-Djava.rmi.server.hostname=121.36.175.1 //IP 地址需要与外网访问地址一致

// 下面参数为使用用户名密码的方式启用远程访问时的参数，不启用时可以不增加

-Dcom.sun.management.jmxremote.authenticate=true

-Dcom.sun.management.jmxremote.access.file=/home/jmxremote/jmxremote.access

-Dcom.sun.management.jmxremote.password.file=/home/jmxremote/jmxremote.password"
```

- 开启 JMX 远程访问的用户密码权限配置

如果需要使用用户名密码的 JMX 远程访问方式时，可以通过下面的方式建立访问权限控制文件，并放置到/home/jmxremote 目录下。

```
// 权限控制文件 jmxremote.access 内容

controlRole readwrite

create javax.management.monitor.*,javax.management.timer.*

unregister

// 权限控制文件 jmxremote.password 内容

controlRole R&D
```

设置权限控制文件为只读模式

```
[root@server ~]# chmod 400 jmxremote.access

[root@server ~]# chmod 400 jmxremote.password
```

1.3.2.1.4 需要将 Tomcat 的 JMX 监听的 TCP 端口加入到系统防火墙规则

1) 检查 JMX 监听的 TCP 端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) JMX 监听的 TCP 端口加入到系统防火墙规则方法

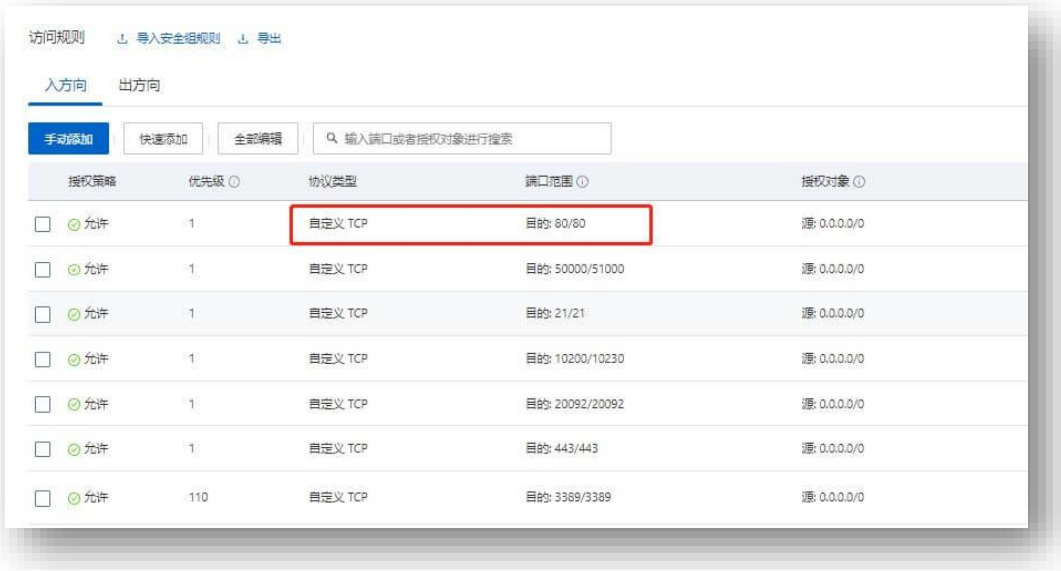
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 JMX 监听端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:8162/8162（或自定义端口号）



4) 云服务器开启 JMX 监听端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.3.2.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 Tomcat v8.x 及以上版本

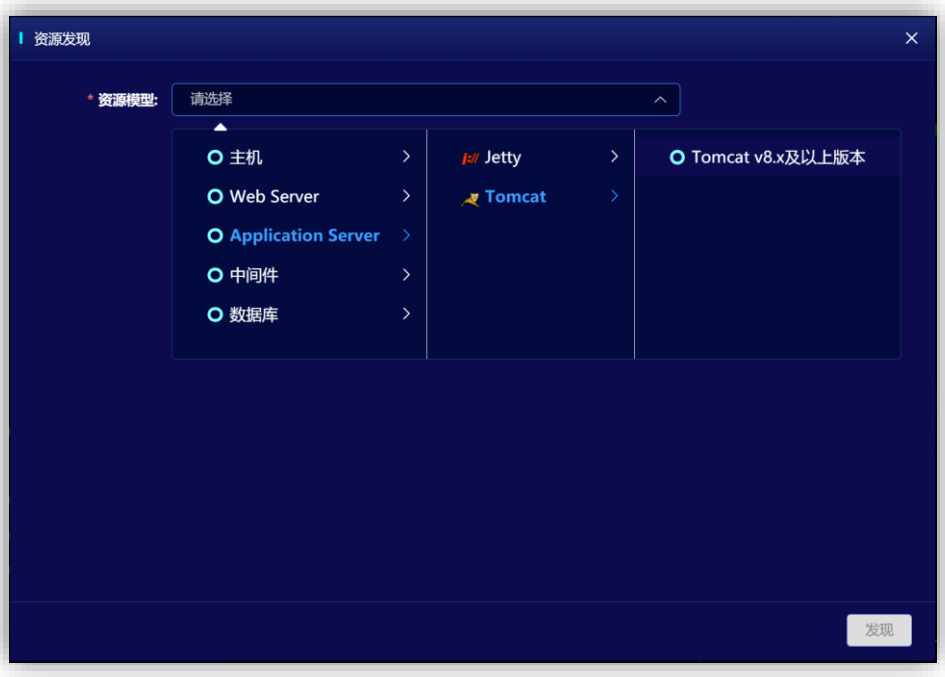


图 2-27 资源发现页面

- 从下面的窗口中输入 IP 地址、端口，用户名（对应 jmx 中权限模式的用户名）和密码（对应 jmx 中权限模式的密码），选择主机模型后输入对应的连接信息。

图 2-28 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-29 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-30 资源概览页

1.4 中间件

1.4.1 RabbitMQ 集群

1.4.1.1 发现前提

1.4.1.1.1 如果 RabbitMQ 所在主机未被发现，请先检查主机是否满足发现前提

1.4.1.1.2 需要开启 RabbitMQ 管理插件、开启 Developer 用户管理权限

以下的操作步骤及配置方法是在 Linux 环境下，Windows 环境下的配置方法相同。

1) 检查 RabbitMQ 是否开启管理插件

```
[root@server ~]# ./rabbitmq-plugins list | grep rabbitmq_management
```

2) RabbitMQ 开启管理插件方法

```
[root@server ~]# ./rabbitmq-plugins enable rabbitmq_management
```

3) 检查 Developer 用户是否具备管理权限

```
[root@server ~]# ./rabbitmqctl list_users

Listing users ...

user tags

developer [administrator]
```

4) 开启 Developer 用户管理权限的方法

```
[root@server ~]# ./rabbitmqctl add_user developer 123456

[root@server ~]# ./rabbitmqctl set_user_tags developer administrator

[root@server ~]# ./rabbitmqctl set_permissions -p / developer ".*" ".*" ".*"
```

1.4.1.1.3 需要将管理插件的 TCP 端口加入到系统防火墙规则

1) 检查管理插件的 TCP 端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) 管理插件的 TCP 端口加入到系统防火墙规则方法

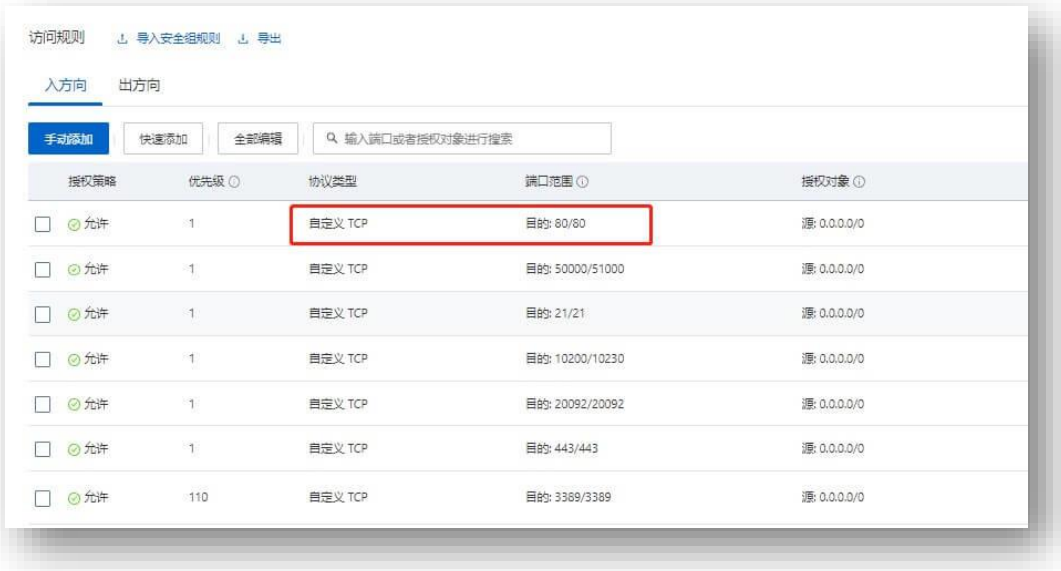
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:8162/8162（或自定义端口号）



4) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.4.1.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 RabbitMQ 集群-v3.8 及以上版本

图 2-31 资源发现页面

- 从下面的窗口中输入 IP 地址、端口、用户名、密码，点击发现。

图 2-32 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

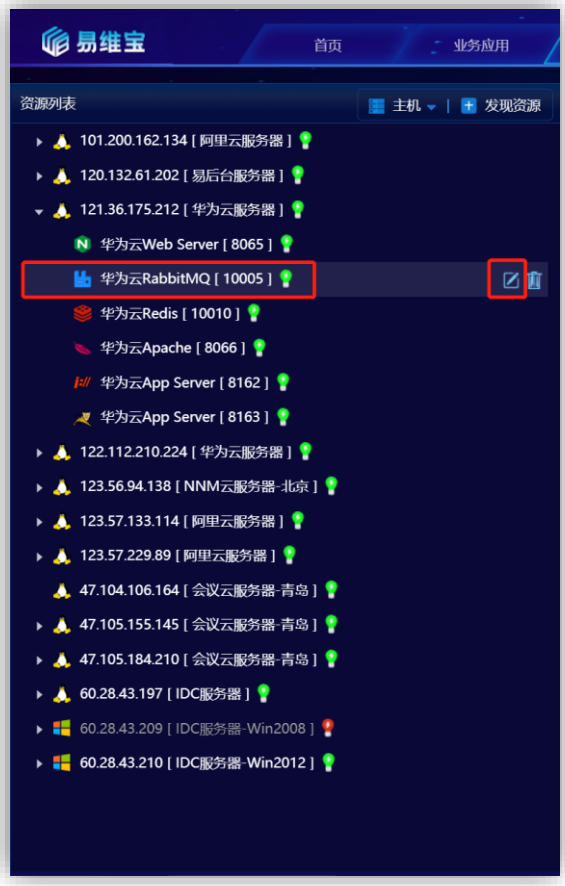


图 2-33 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-34 资源概览页

1.4.1.3 FAQ

1) 如何搭建 RabbitMQ 集群?

RabbitMQ 安装及集群搭建，请参考如下链接地址。

https://www.jianshu.com/p/b6bc3cba69c2

1.4.2 ElasticSearch 集群

1.4.2.1 发现前提

1.4.2.1.1 如果 ElasticSearch 所在主机未被发现，请先检查主机是否满足发现前提

1.4.2.1.2 安装好集群后无需过多配置

1.4.2.1.3 需要将 ElasticSearch 集群主节点 HTTP 端口加入到系统防火墙规则

1) 检查 ElasticSearch 集群主节点 HTTP 端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) ElasticSearch 集群主节点 HTTP 端口加入到系统防火墙规则方法

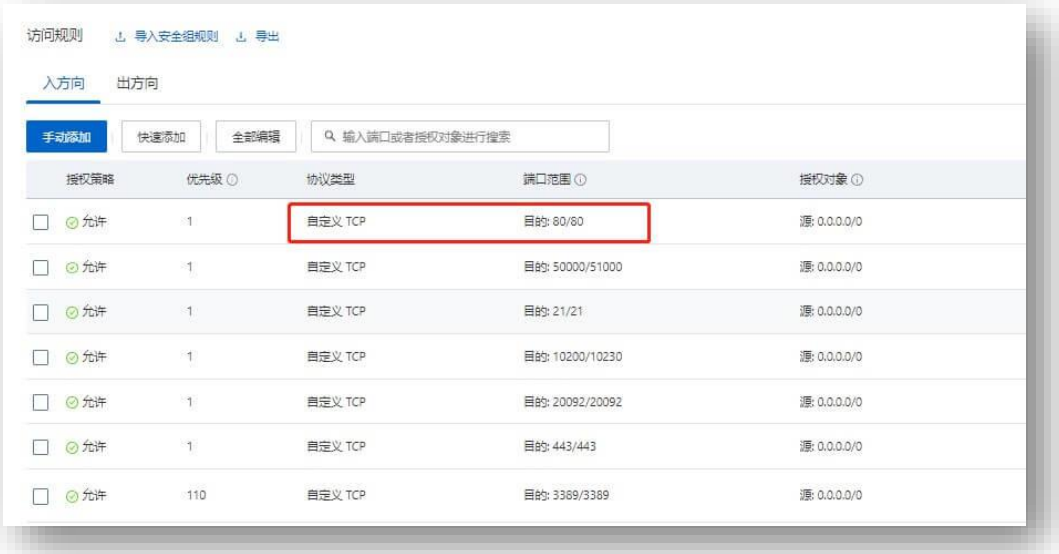
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:9200/9200（或自定义端口号）



4) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.4.2.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 ElasticSearch 集群监控模型

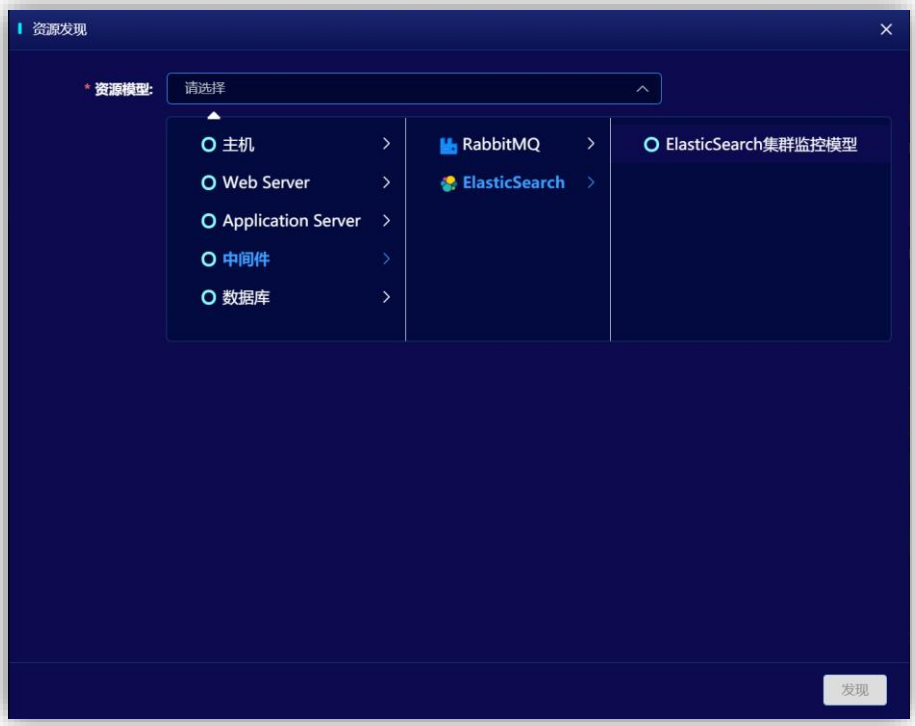


图 2-35 资源发现页面

- 从下面的窗口中输入主节点 IP、主节点端口后，点击发现。

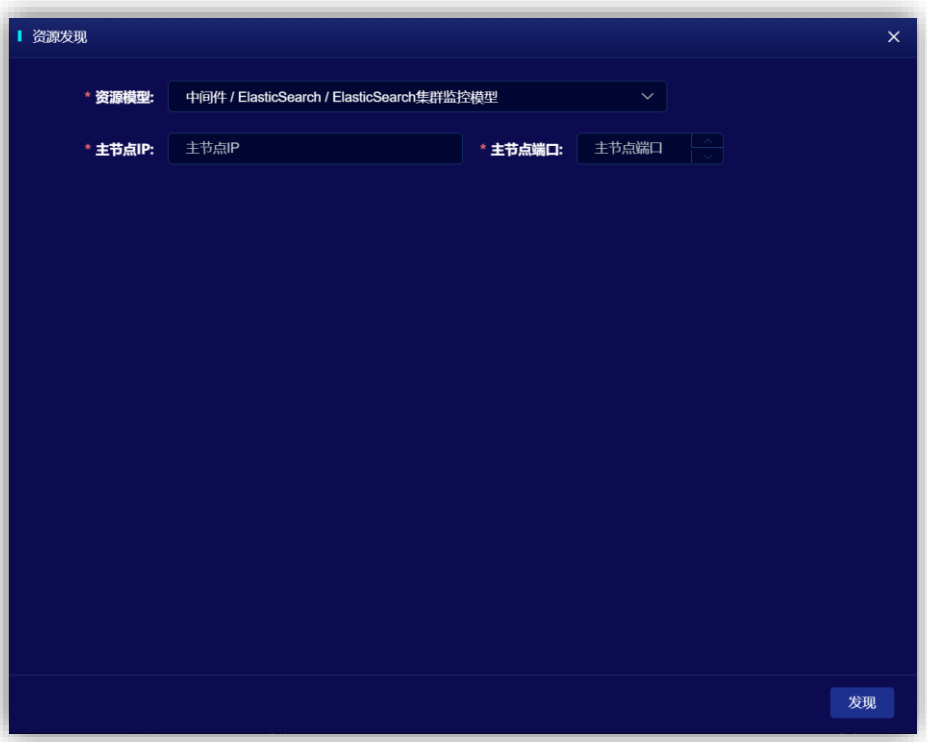


图 2-36 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-37 发现资源后的资源列表

- 点击资源后，进入资源概览页

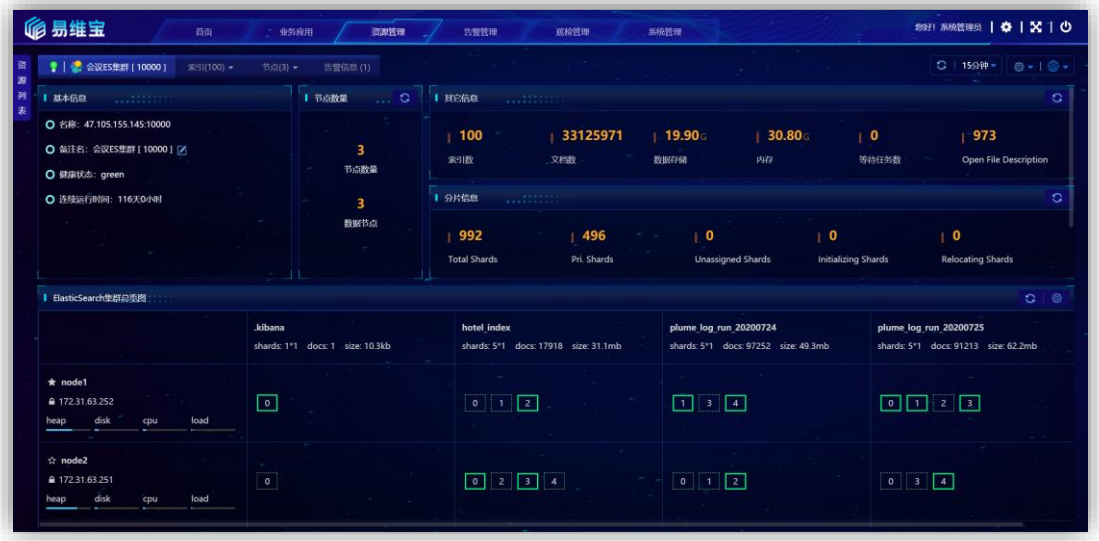


图 2-38 资源概览页

1.4.2.3 FAQ

1) 如何搭建 ElasticSearch 集群?

Es 集群的搭建，请参考如下链接地址。

https://www.jianshu.com/p/57c3061bb6cb

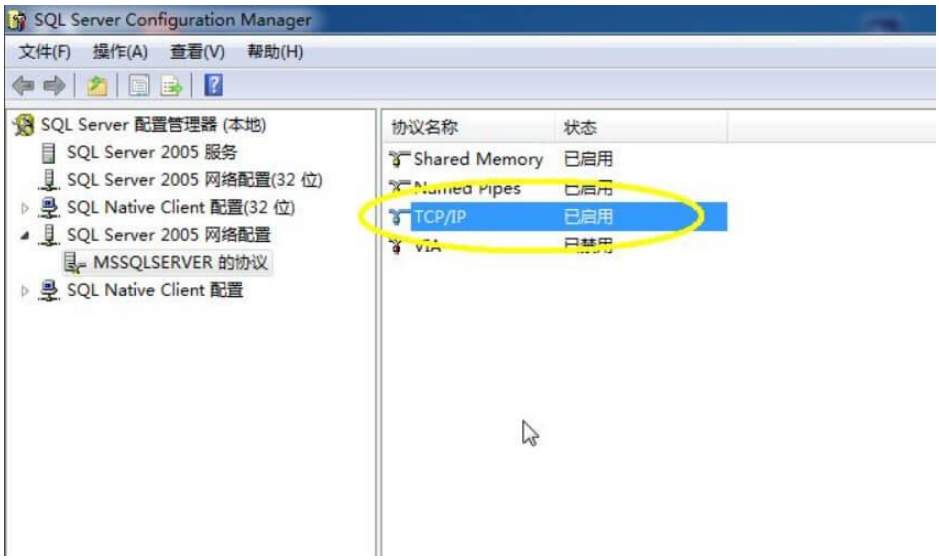
1.5 数据库

1.5.1 SQLSERVER

1.5.1.1 发现前提

1.5.1.1.1 如果 SQLServer 数据库所在主机未被发现，请先检查主机是否满足发现前提

1) 检查 SQLServer 的 TCP/IP 访问协议是否开启



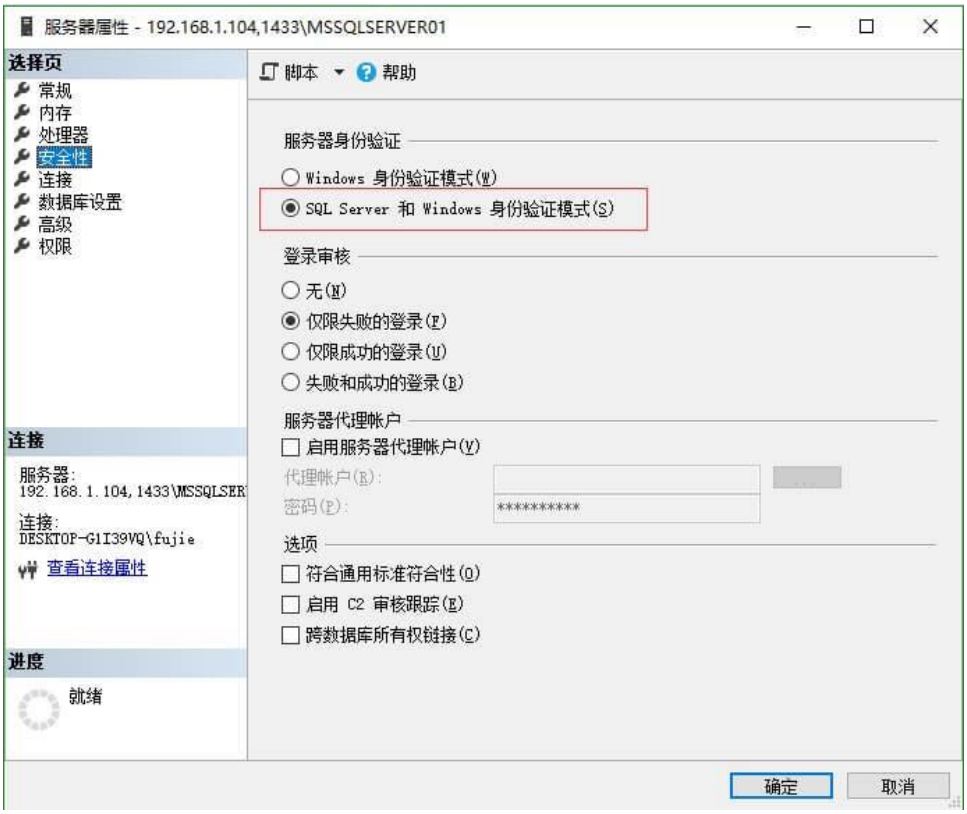
2) 开启 SQLServer 的 TCP/IP 访问协议是否方法

- 具体操作方法请访问下面的链接:

  https://www.cnblogs.com/fengjingfei/p/13021680.html

3) 检查连接用户是否开启混合身份验证模式和 sysadmin 权限

- 进入连接用户的安全性属性中，查看服务器身份验证是否为下面图的设置



4) 开启连接用户是否开启混合身份验证模式和 sysadmin 权限方法

- 具体操作方法请访问下面的链接：

https://www.fujieace.com/mssql/create-login.html

1.5.1.1.2 需要将 SQLServer 数据库的 TCP/IP 端口加入到系统防火墙规则

1) 检查 SQLServer 数据库的 TCP/IP 端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) SQLServer 数据库的 TCP/IP 端口加入到系统防火墙规则方法

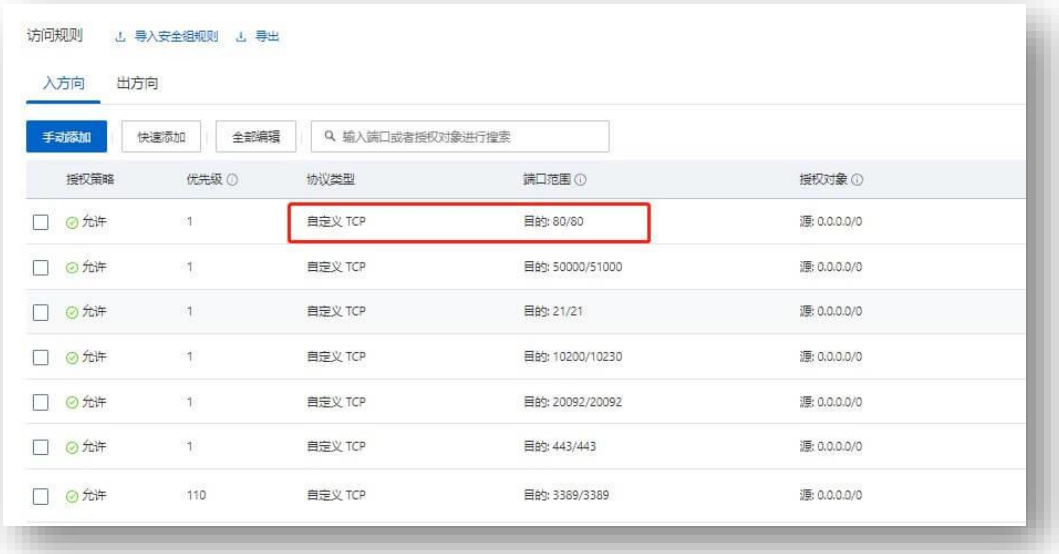
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:1433/1433（或自定义端口号）



4) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.5.1.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 SQL Server 2008 及以上版本

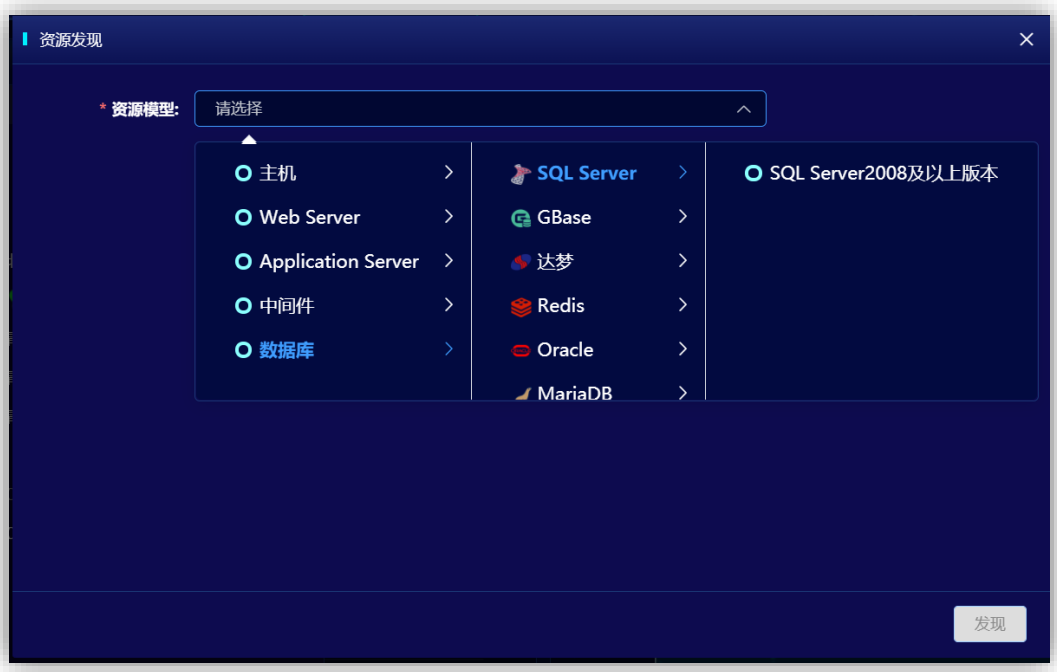


图 2-39 资源发现页面

- 从下面的窗口中输入数据库 IP 地址、数据库端口、用户名、密码，查询超时(秒)及主机连接信息。

图 2-40 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-41 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-42 资源概览页

1.5.1.3 FAQ

1) 如何验证监控应用服务器与被监控端主机及资源是否正常连接？在监控应用服务器上使用 root 命令运行 telnet 验证。

```
[root@server ~]# telent 192.168.0.10 1433
```

2) 如何开启 SQLSERVER 用户的远程访问?

参见如下网页开启远程访问
https://www.cnblogs.com/weizhengLoveMayDay/p/3267756.html

1.5.2 GBase

支持 GBase 8s 8.8 版本及以上的版本监控。

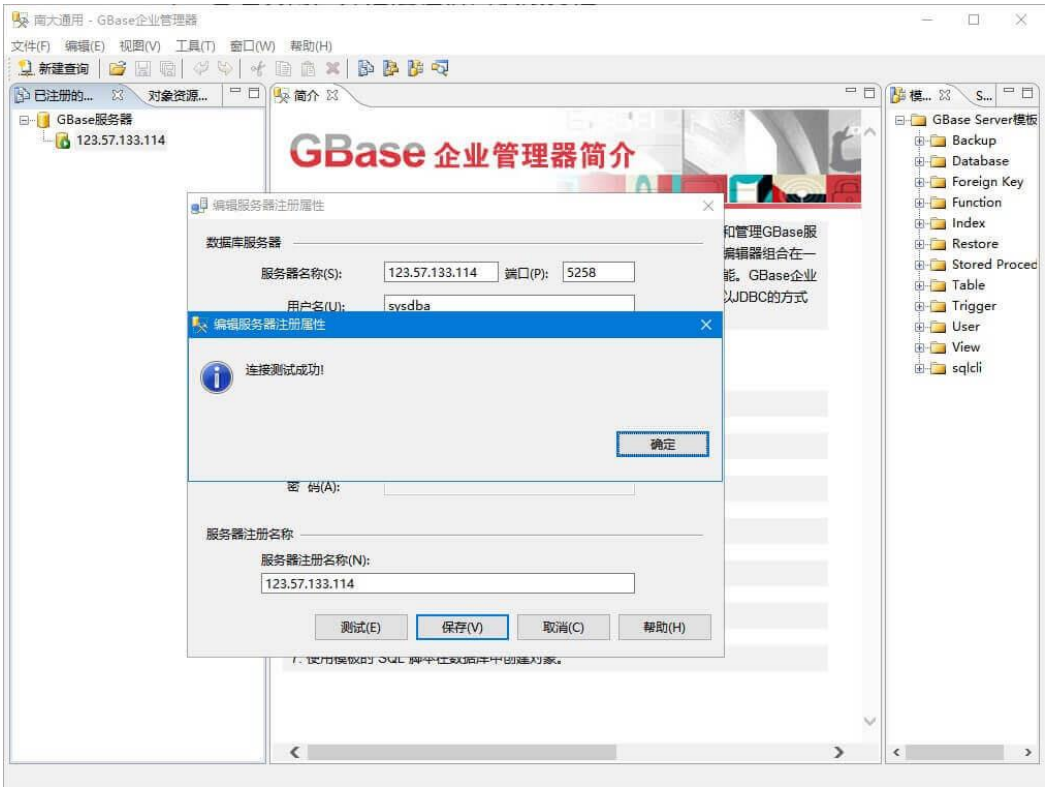
1.5.2.1 发现前提

1.5.2.1.1 如果 GBase 数据库所在主机未被发现，请先检查主机是否满足发现前提

1.5.2.1.2 需要开启管理员用户远程访问权限、开启慢日志

1) 检查管理员用户是否具有远程访问权限

使用 GBase 企业管理器工具远程连接验证



2) 管理员用户开启远程访问权限方法

```
[root@mqnode2 bin]# ./sqlcli -usysdba -pGBase8sV8316

sqlcli: [Warning] Using a password on the command line interface can be insecure.

Welcome to the GBase SQLCLI. Commands end with ; or g.

Your GBase connection id is 40978

Server version: 8.8 -log build 200
```

```
Copyright (c) 2004-2018, GBase. All rights reserved.

Type 'help;' or 'h' for help. Type 'c' to clear the current input statement.

sqlcli>
sqlcli>
sqlcli>
sqlcli> set password for 'sysdba'@'%'=password('GBase8sV8316');
Query OK, 0 rows affected, 1 warning (0.01 sec)

sqlcli> flush privileges;
Query OK, 0 rows affected (0.01 sec)
```

3) 检查数据库是否开启慢日志

```
[root@mqnode2 bin]# ./sqlcli -usysdba -pGBase8sV8316
sqlcli> show variables like '%slow_query_log%';
| Variable_name | Value |
+--------------------------+-----------------------------------------------------+
| slow_query_log | ON |
| slow_query_log_file | /opt/GBase/Server/data/iz2zehdkhnyvzjegcs1i4gz-slow.log |
+--------------------------+-----------------------------------------------------+
5 rows in set (0.00 sec)
```

4) 数据库开启慢日志方法

- 在 /opt/GBase/Server/etc/gs.cnf 配置文件中增加如下配置

```
[gbased]

slow_query_log = 1

long_query_time = 10

log_output='table'
```

- 重新启动 GBase 服务

```
[root@mqnode2 bin]# ./gbase.server restart
```

1.5.2.1.3 需要将 GBase 数据库的连接端口加入到系统防火墙规则

1) GBase 数据库的连接端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) 检查 GBase 数据库的连接端口加入到系统防火墙规则方法

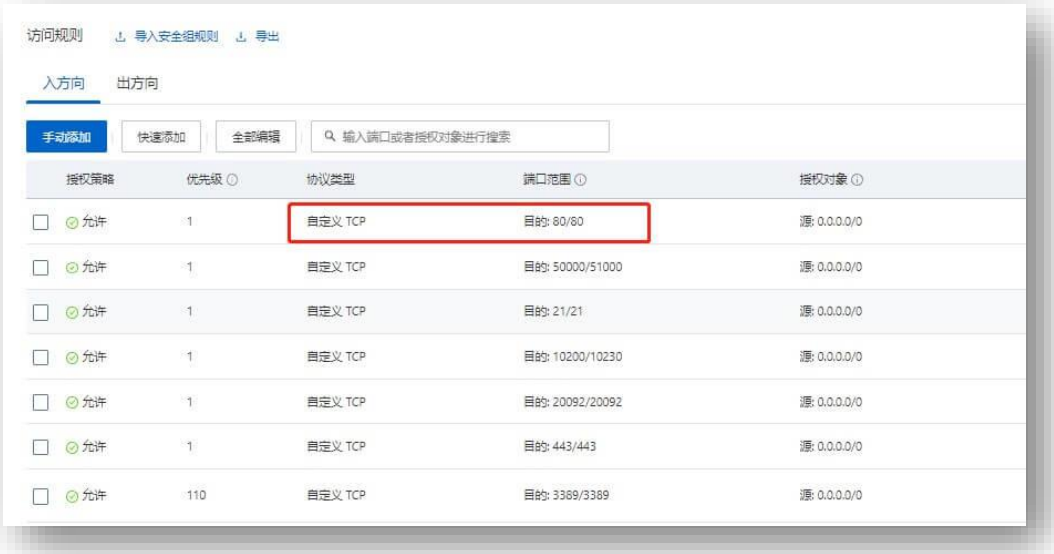
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:5258/5258（或自定义端口号）



4) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.5.2.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 GBase 8S v8.x 及以上版本

图 2-43 资源发现页面

- 从下面的窗口中输入 IP 地址、端口、用户名\密码、选择主机模型后输入对应的连接信息，点击发现。

图 2-44 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

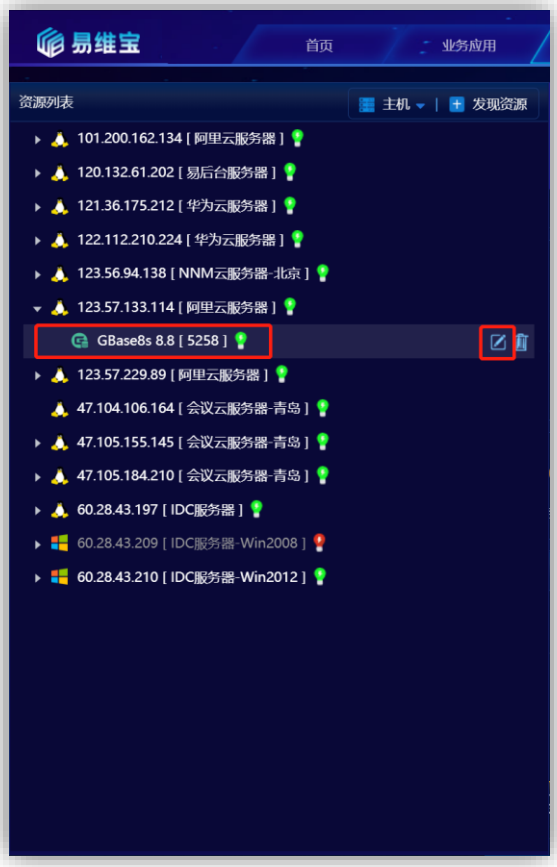


图 2-45 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-46 资源概览页

1.5.3 达梦

目前支持达梦 7、达梦 8（8.1.1 及以上版本）数据库，具体版本差异请联系达梦数据库公司或达梦数据库官网。

1.5.3.1 发现前提

1.5.3.1.1 如果达梦数据库所在主机未被发现，请先检查主机是否满足发现前提

1.5.3.1.2 需要连接用户具备管理权限

- 具体操作依据达梦数据库版本不同，请依据数据库厂商的手册进行设置
  https://www.10qianwan.com/articledetail/627078.html

1.5.3.1.3 需要将达梦数据库的连接端口加入到系统防火墙规则

1) 达梦数据库的连接端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) 检查达梦数据库的连接端口加入到系统防火墙规则方法

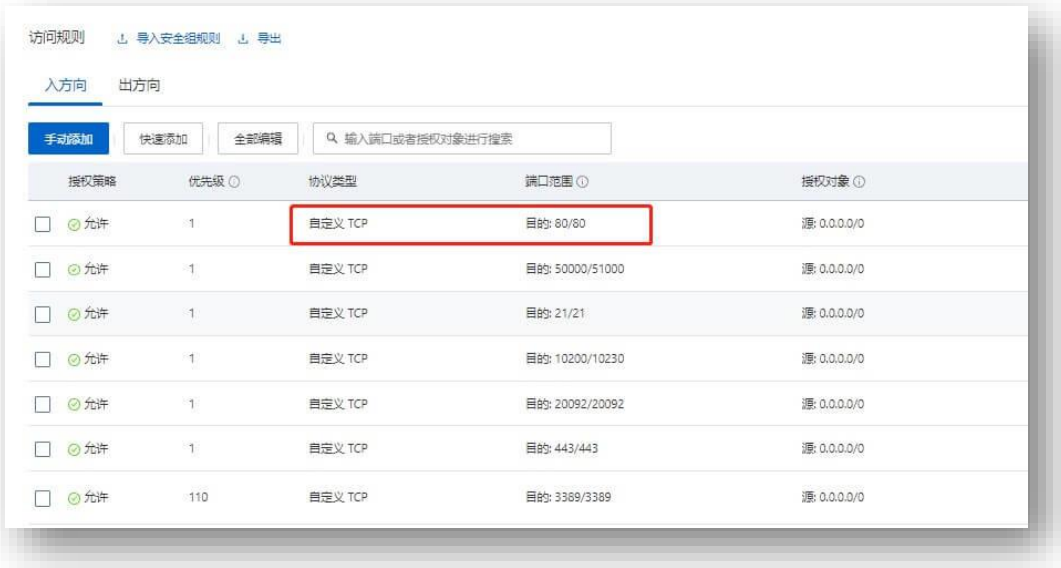
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:5336/5336（或自定义端口号）



4) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.5.3.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 MariaDB v10.x 及以上版本

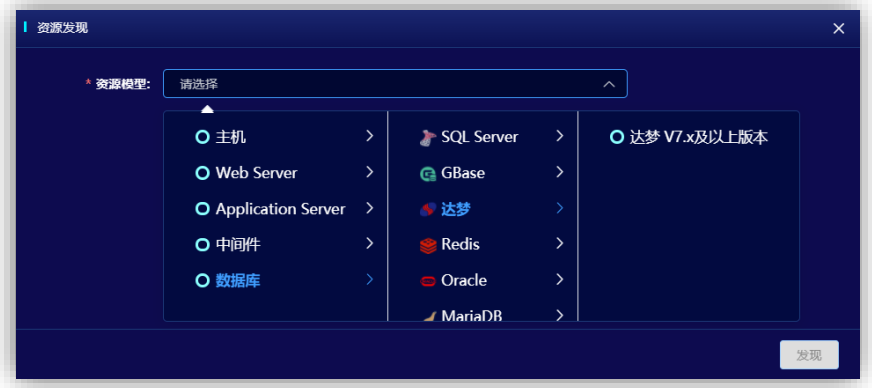


图 2-47 资源发现页面

- 从下面的窗口中输入 IP 地址、端口、用户名、密码后，输入主机的连接信息，点击发现。

图 2-48 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-49 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-50 资源概览页

1.5.4 Redis

1.5.4.1 发现前提

1.5.4.1.1 如果 Redis 数据库所在主机未被发现，请先检查主机是否满足发现前提

1.5.4.1.2 需要开启 Redis 数据库授权访问、验证 redis-info 命令是否可用

1) 验证是否开启 Redis 数据库授权访问

```
[root@server ~]# ./redis-cli -p 10005

127.0.0.1:10005> auth 1qa2ws3ed@123456

OK
```

2) 开启 Redis 数据库授权访问方法

打开 redis.conf 配置文件/usr/local/redis/bin/redis.conf 或/etc/redis.conf，开启 requirepass 配置

```
[root@server ~]# ./redis-cli -p 10005
```

```
127.0.0.1:10005> info

# Server

redis_version:5.0.5

redis_git_sha1:00000000

redis_git_dirty:0

redis_build_id:5f65f28f6bb0b514

redis_mode:cluster

os:Linux 3.10.0-693.2.2.el7.x86_64 x86_64

arch_bits:64

multiplexing_api:epoll

atomicvar_api:atomic-builtin

gcc_version:4.8.5

.....
```

3) 验证 redis-info 命令是否可用

打开 redis.conf 配置文件/usr/local/redis/bin/redis.conf 或/etc/redis.conf，开启 requirepass 配置

```
requirepass 12345678
```

1.5.4.1.3 需要将 Redis 数据库的连接端口加入到系统防火墙规则

1) 检查 Redis 数据库的连接端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向             名称
----------------------------------------------------------------------
33060  TCP      启用      入站       Port 33060
3306   TCP      启用      入站       Port 3306
8879   UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站       zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站       zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站       zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向             名称
----------------------------------------------------------------------
33060  TCP      启用      入站       Port 33060
3306   TCP      启用      入站       Port 3306
8879   UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站       zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站       zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站       zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站       zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) Redis 数据库的连接端口加入到系统防火墙规则方法

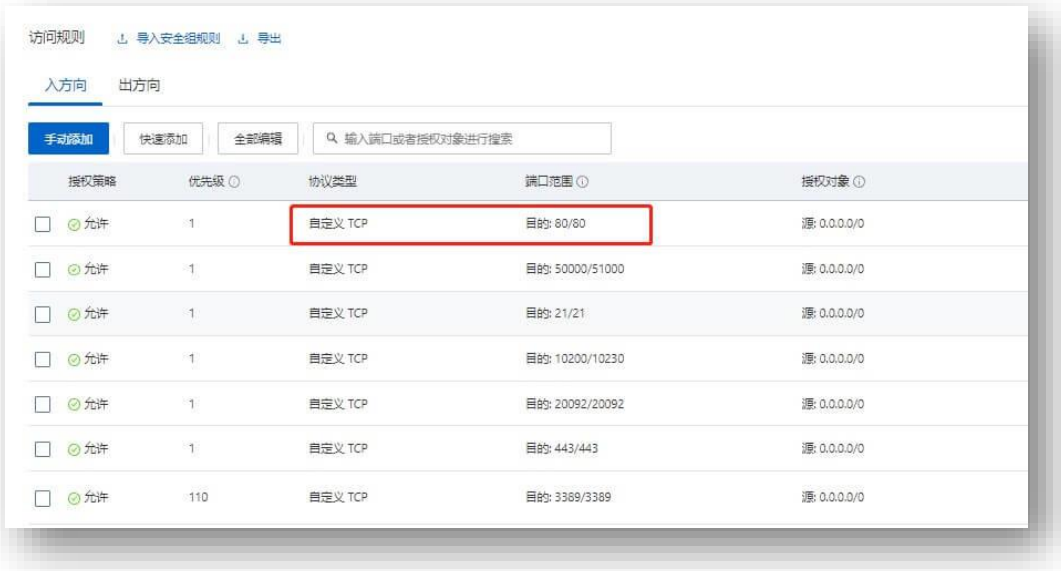
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:6379/6379（或自定义端口号）



4) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.5.4.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 Redis v5.x 及以上版本单机监控模型

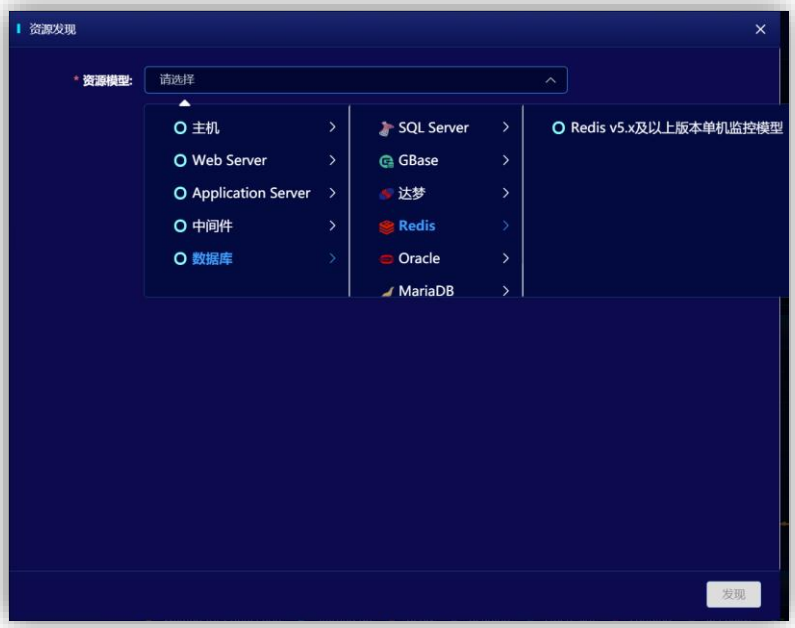


图 2-51 资源概览页

- 从下面的窗口中输入 IP 地址、端口、密码输入对应的主机连接信息后点击发现。

图 2-52 资源概览页

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

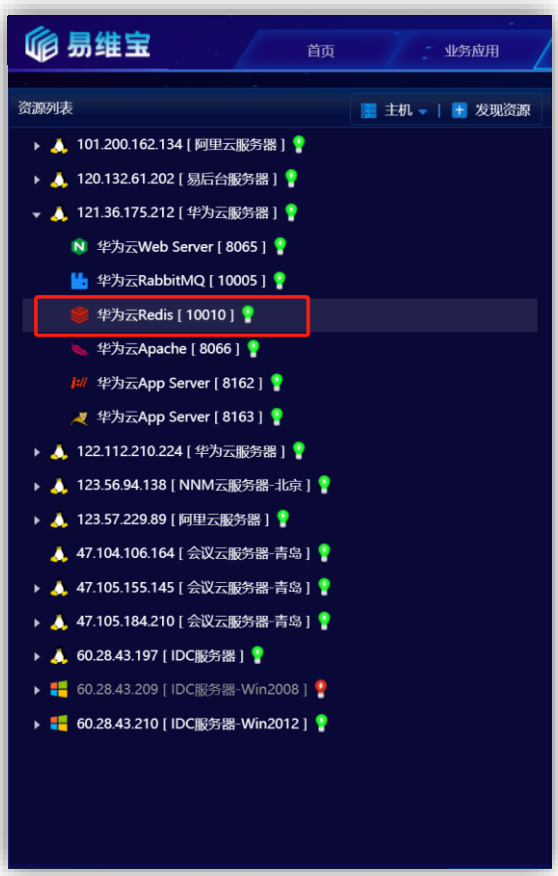


图 2-53 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-54 资源概览页

1.5.4.3 FAQ

1) 如何设置 Redis 的授权密码?

请参考如下链接地址。

https://www.cnblogs.com/rianley/p/11679141.html

1.5.5 PostgreSQL

1.5.5.1 发现前提

1.5.5.1.1 如果 PostgreSQL 所在主机未被发现，请先检查主机是否满足发现前提 windows 或 linux

1.5.5.1.2 2. 需要开启用户管理员权限、开启 pg_stat_statements 模块、开启远程访问

以下的操作步骤及配置方法是在 Linux 环境下，Windows 环境下的配置方法相同。

1) 检查及创建超级管理员权限用户方法

具体操作请参见下面的链接地址:

https://www.cnblogs.com/zhoujinyi/p/10939715.html

2) 检查是否开启 pg_stat_statements 模块

使用管理工具执行下面命令

```
select * from pg_stat_statements;
```

3) 开启 pg_stat_statements 模块方法

- 在 postgresql.conf 中加入以下配置加载 pg_stat_statements 模块

```
shared_preload_libraries = 'pg_stat_statements'

pg_stat_statements.max = 10000

pg_stat_statements.track = all
```

- 数据库管理工具中创建扩展

```
postgres=# create extension pg_stat_statements;

CREATE EXTENSION
```

- 重启数据库

```
[root@server ~]# pg_ctl restart
```

- 检查是否开启远程访问

使用客户端管理工具建立连接测试是否允许建立连接

- 开启远程访问方法

在 pg_hba.conf 中加入以下配置

```
host all all 0.0.0.0/0 md5
```

重启数据库

```
[root@server ~]# pg_ctl restart
```

1.5.5.1.3 需要将 PostgreSQL 数据库的连接端口加入到系统防火墙规则

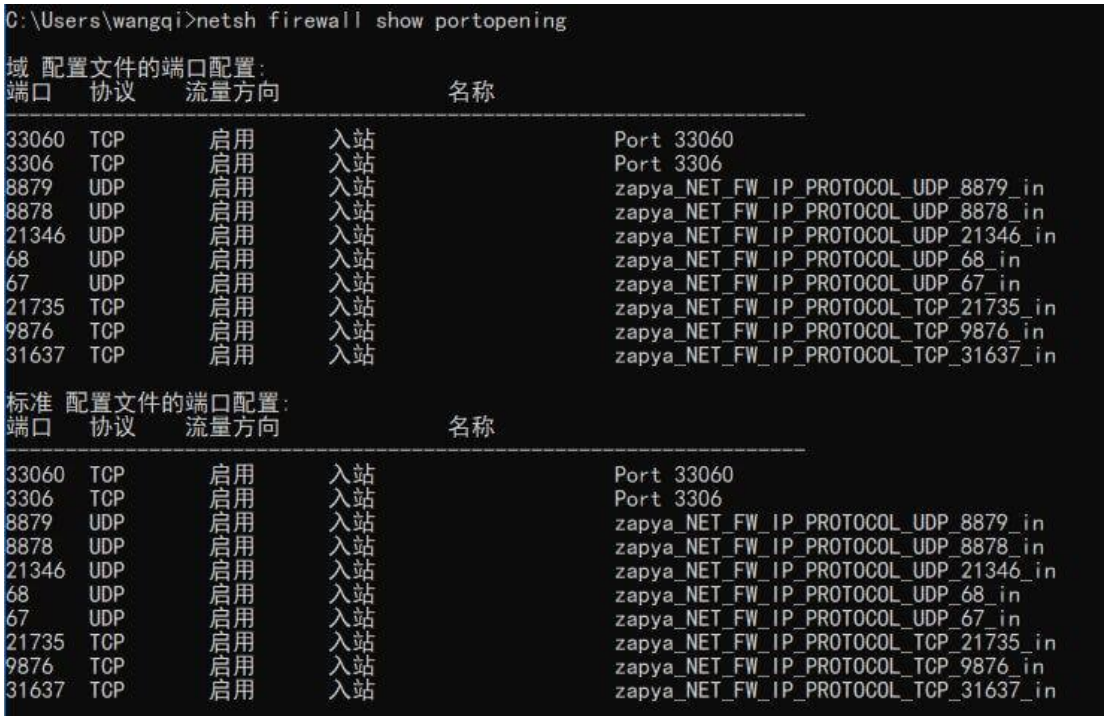
1) 检查 PostgreSQL 数据库的连接端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```



2) PostgreSQL 数据库的连接端口加入到系统防火墙规则方法

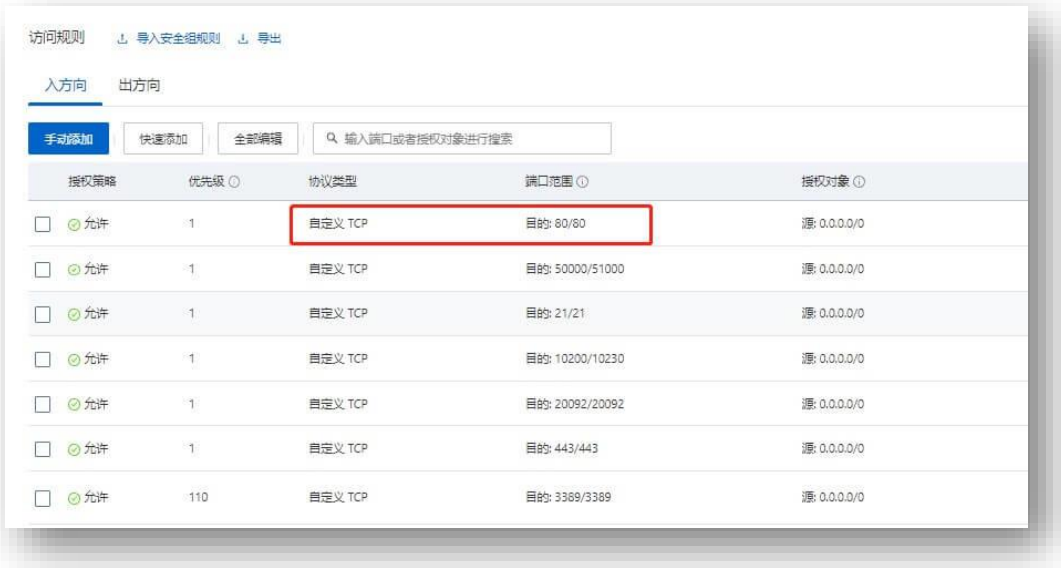
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:5432/5432（或自定义端口号）



4) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.5.5.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 PostgreSQL v11.x 及以上版本

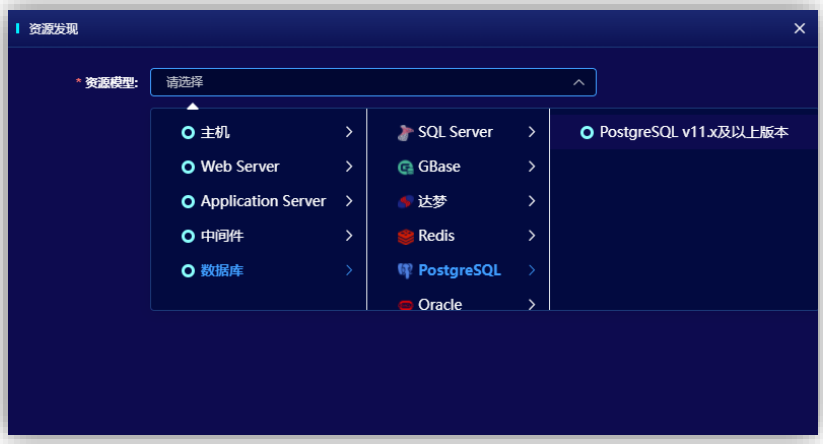


图 2-55 资源发现页面

- 从下面的窗口中输入 IP 地址、端口、选择主机模型后输入对应的连接信息。

图 2-56 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-57 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-58 资源概览页

1.5.6 Oracle

1.5.6.1 发现前提

1.5.6.1.1 如果 Oracle 所在主机未被发现，请先检查主机是否满足发现前提

windows 或 linux

1.5.6.1.2 需要设置用户的 DBA 的权限

1) 检查用户是否具备 DBA 权限

使用 Oracle 管理工具执行下面的查询语句

```
select * from dba_users;
```

2) 开启用户 DBA 权限方法

具体操作方法请使用下面的链接地址:

https://blog.csdn.net/baidu_35901646/article/details/104280809

1.5.6.1.3 需要将 Oracle 数据库的连接端口加入到系统防火墙规则

1) Oracle 数据库的连接端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) Oracle 数据库的连接端口加入到系统防火墙规则方法

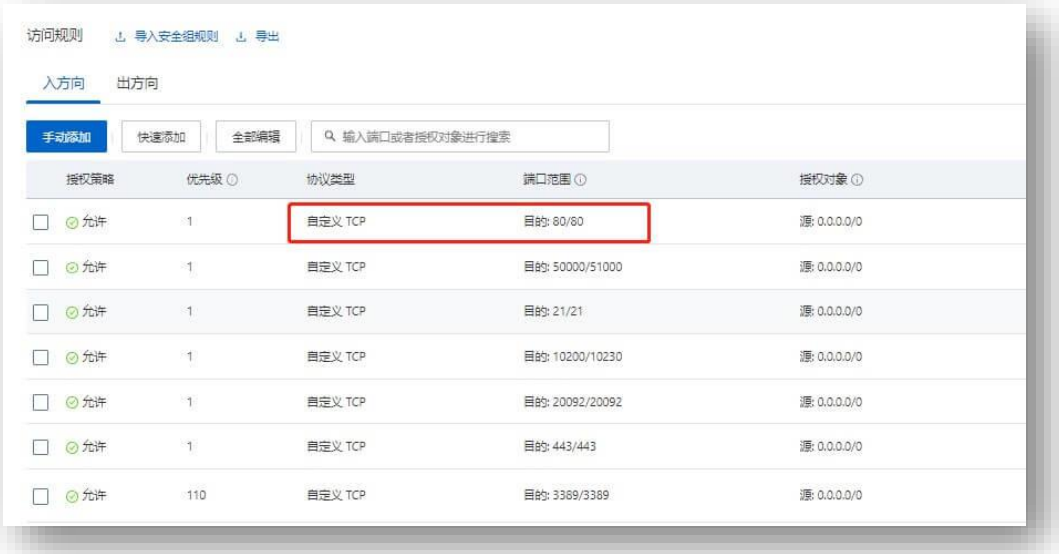
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:1521/1521（或自定义端口号）



4) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.5.6.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 Oracle v11.x 及以上版本单机监控模型

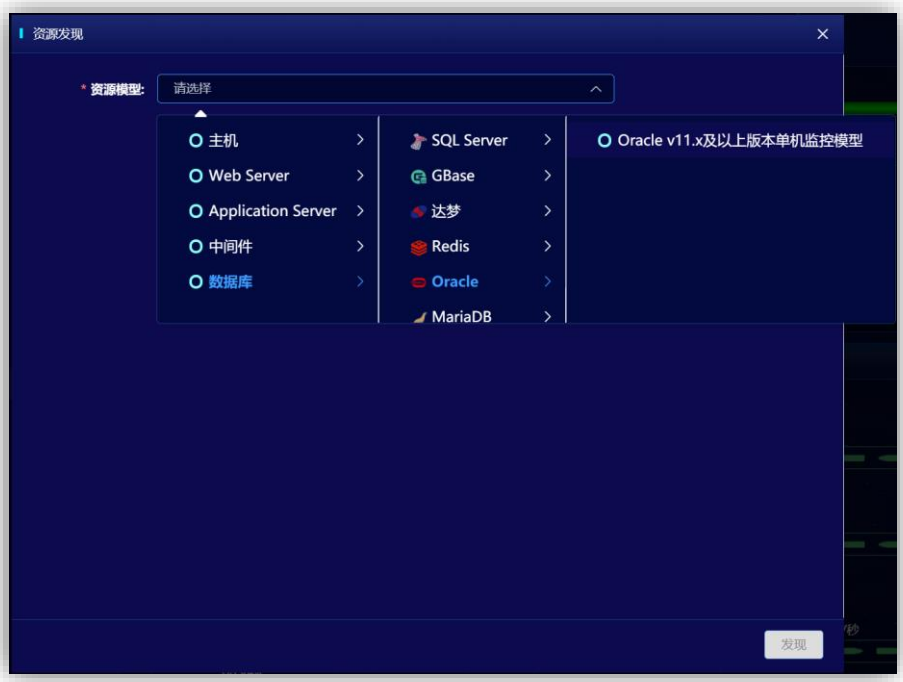


图 2-59 资源概览页

- 从下面的窗口中输入数据库 IP 地址、数据库端口、SID、用户名、密码，选择主机模型后输入对应的连接信息，点击发现完成。

图 2-60 资源概览页

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

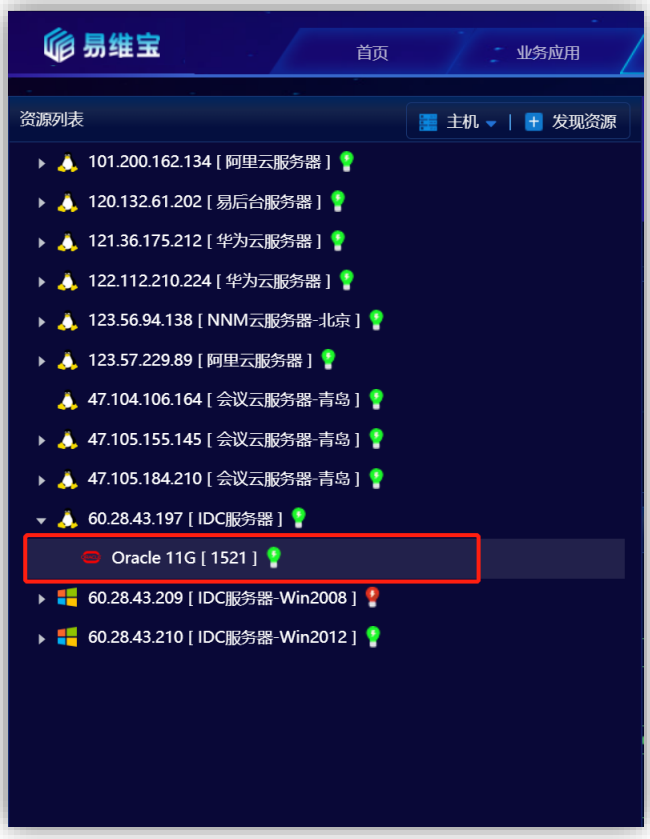


图 2-61 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-62 资源概览页

1.5.7 MariaDB

1.5.7.1 发现前提

1.5.7.1.1 如果 MariaDB 所在主机未被发现，请先检查主机是否满足发现前提

windows 或 linux

1.5.7.1.2 需要设置用户的远程访问及所有权限、开启慢日志

以下的操作步骤及配置方法是在 Linux 环境下，Windows 环境下的配置方法相同。

4) 检查用户的是否具备远程访问及所有权限

```
MariaDB [mysql]> use mysql;

MariaDB [mysql]> select * from user where user='monitor_user';
```

5) 开启用户的是否具备远程访问及所有权限方法

使用具有 GRANT 权限的用户登录 mysql，执行如下语句

```
GRANT ALL PRIVILEGES ON *.* TO ' monitor_user'@'%' IDENTIFIED BY '1234';

FLUSH PRIVILEGES;
```

6) 检查数据库是否开启慢日志

```
MariaDB [mysql]> show variables like '%slow_query_log%';

+---------------------+------------------+

| Variable_name | Value |

+---------------------+------------------+

| slow_query_log | ON |

| slow_query_log_file | mariadb-slow.log |

+---------------------+------------------+
```

7) 开启数据库慢日志方法

在 my.ini 或 my.cnf 配置文件中添加下面的配置

```
[mysqld]

slow_query_log=1

long_query_time=10

log_output='table'
```

重启数据库

```
[root@server ~]# service mysqld restart
```

1.5.7.1.3 需要将 MariaDB 数据库的连接端口加入到系统防火墙规则

5) 检查 MariaDB 数据库的连接端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向              名称
----------------------------------------------------------------------
33060  TCP      启用      入站        Port 33060
3306   TCP      启用      入站        Port 3306
8879   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站        zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站        zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

6) MariaDB 数据库的连接端口加入到系统防火墙规则方法

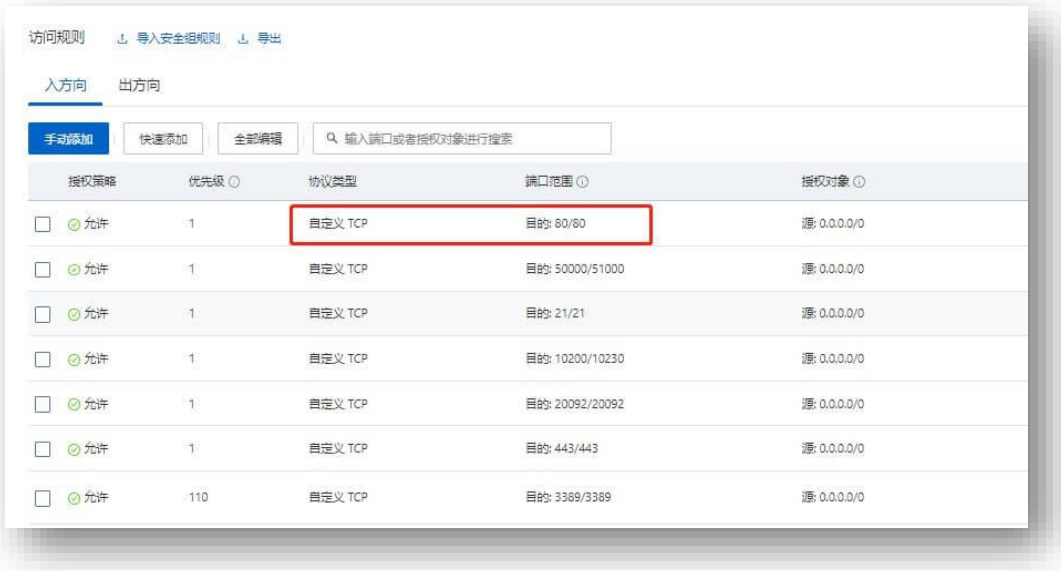
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

7) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:3306/3306（或自定义端口号）



8) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.5.7.2 发现资源

用户登录系统后。顺序进行如下操作。

- 点击资源管理菜单（见图 2-1）
- 点击左侧资源列表（见图 2-2）
- 在资源模型下拉列表中选择 MariaDB v10.x 及以上版本

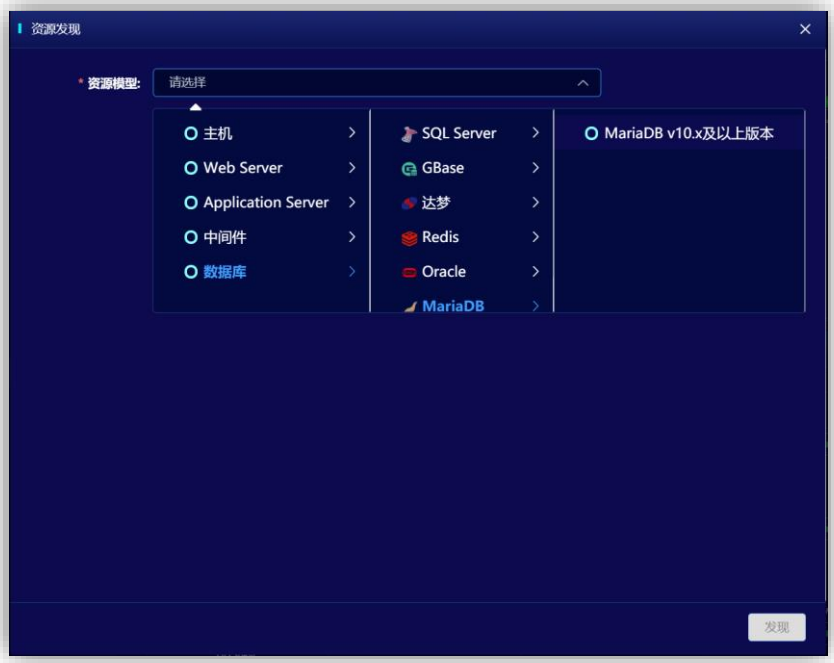


图 2-63 资源发现页面

- 从下面的窗口中输入 IP 地址、端口、选择主机模型后输入对应的连接信息。

图 2-64 资源发现页面

- 资源发现后，会在资源列表中多出刚刚发现的资源，可以通过右侧的编辑按钮修改发现资源的名称。

图 2-65 发现资源后的资源列表

- 点击资源后，进入资源概览页

图 2-66 资源概览页

1.5.8 MySQL

1.5.8.1 发现前提

1.5.8.1.1 如果 MySQL 所在主机未被发现，请先检查主机是否满足发现前提

windows 或 linux

1.5.8.1.2 需要设置用户的远程访问及所有权限、开启慢日志

以下的操作步骤及配置方法是在 Linux 环境下，Windows 环境下的配置方法相同。

1) 检查用户的是否具备远程访问及所有权限

```
mysql [mysql]> use mysql;

mysql [mysql]> select * from user where user='monitor_user';
```

2) 开启用户的是否具备远程访问及所有权限方法

使用具有 GRANT 权限的用户登录 mysql，执行如下语句

```
GRANT ALL PRIVILEGES ON *.* TO ' monitor_user'@'%' IDENTIFIED BY '1234';

FLUSH PRIVILEGES;
```

3) 检查数据库是否开启慢日志

```
mysql [mysql]> show variables like '%slow_query_log%';

+---------------------+------------------+

| Variable_name | Value |

+---------------------+------------------+

| slow_query_log | ON |
```

```
| slow_query_log_file | mariadb-slow.log |

+---------------------+------------------+
```

4) 开启数据库慢日志方法

在 my.ini 或 my.cnf 配置文件中添加下面的配置

```
[mysqld]

slow_query_log=1

long_query_time=10

log_output='table'
```

重启数据库

```
[root@server ~]# service mysqld restart
```

1.5.8.1.3 需要将 MySQL 数据库的连接端口加入到系统防火墙规则

1) 检查 MySQL 数据库的连接端口是否加入到系统防火墙规则

- Linux

```
[root@server ~]# firewall-cmd --zone=public --list-ports
```

- Windows

```
C:\Users\wangqi>netsh firewall show portopenin
```

```
C:\Users\wangqi>netsh firewall show portopening

域 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

标准 配置文件的端口配置:
端口   协议     流量方向                名称
----------------------------------------------------------------------
33060  TCP      启用      入站          Port 33060
3306   TCP      启用      入站          Port 3306
8879   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8879_in
8878   UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_8878_in
21346  UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_21346_in
68     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_68_in
67     UDP      启用      入站          zapya_NET_FW_IP_PROTOCOL_UDP_67_in
21735  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_21735_in
9876   TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
31637  TCP      启用      入站          zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
```

2) MySQL 数据库的连接端口加入到系统防火墙规则方法

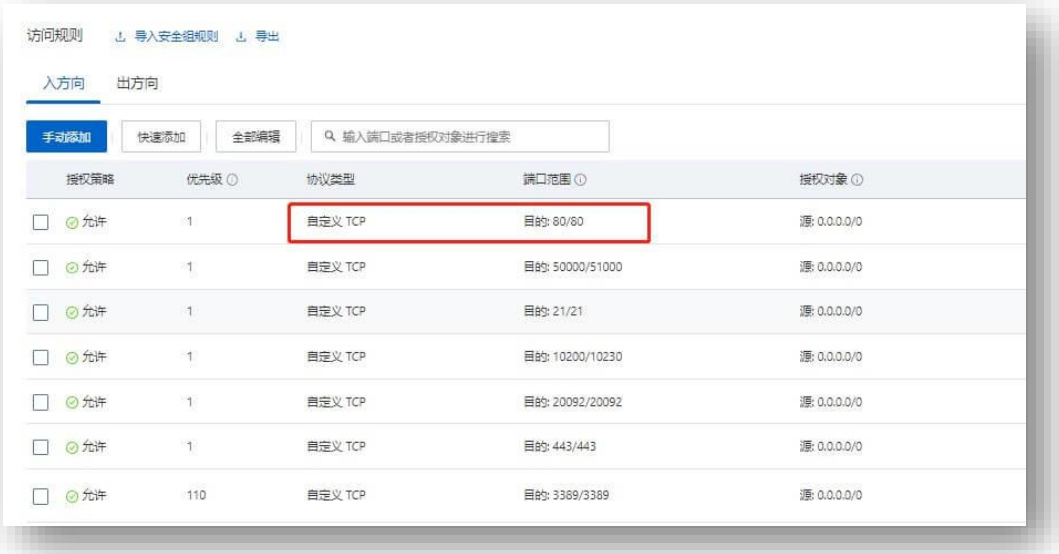
- 具体操作方法请参考如下链接:

  Windows：https://blog.csdn.net/mineskey/article/details/110929469

  Linux：https://www.cnblogs.com/zhaosongbin/p/9765599.html

3) 如果为云服务器，检查是否已经打开 TCP 端口

- 以阿里云云服务器为例，其他云服务器请参考官方说明，下图中的端口范围应该存在，目的:3306/3306（或自定义端口号）



4) 云服务器开启 TCP 端口方法

- 以阿里云云服务器为例，其他云服务器请参考官方说明：

  https://help.aliyun.com/document_detail/25471.html

1.5.8.2 发现资源

与 MariaDB 设置方法一致，参见 2.14.2 章节。

图 2-67 资源概览页

1.6 调整资源模型视图

每个资源发现后，资源概览页面显示默认的视图集合，若需要调整每个资源默认的视图内容，可以点击资源视图右上角的设置按钮更换，也可以创建自定义视图。

1.6.1 更换模型视图

- 点击进入资源管理页面

图 2-68 资源管理页面

- 点击资源视图右上角设置按钮选择视图

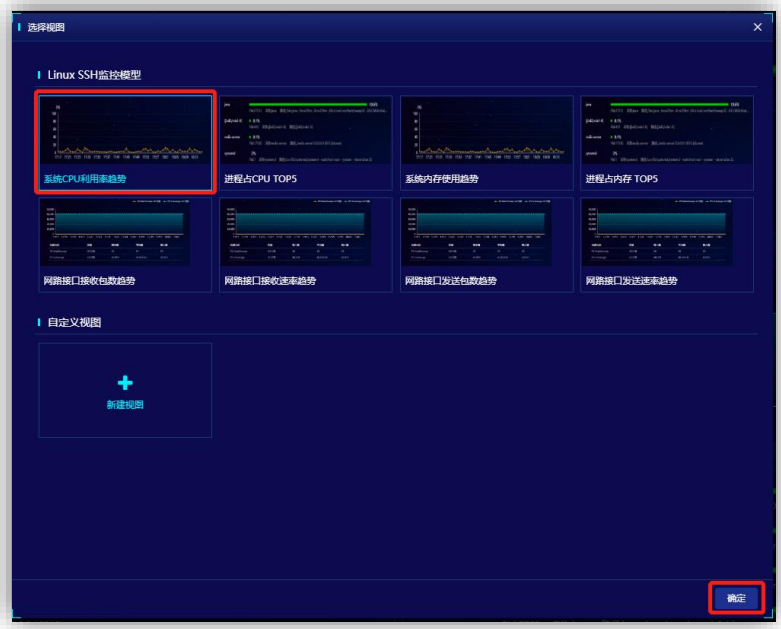


图 2-69 选择视图

1.6.2 自定义视图

- 点击新建视图按钮

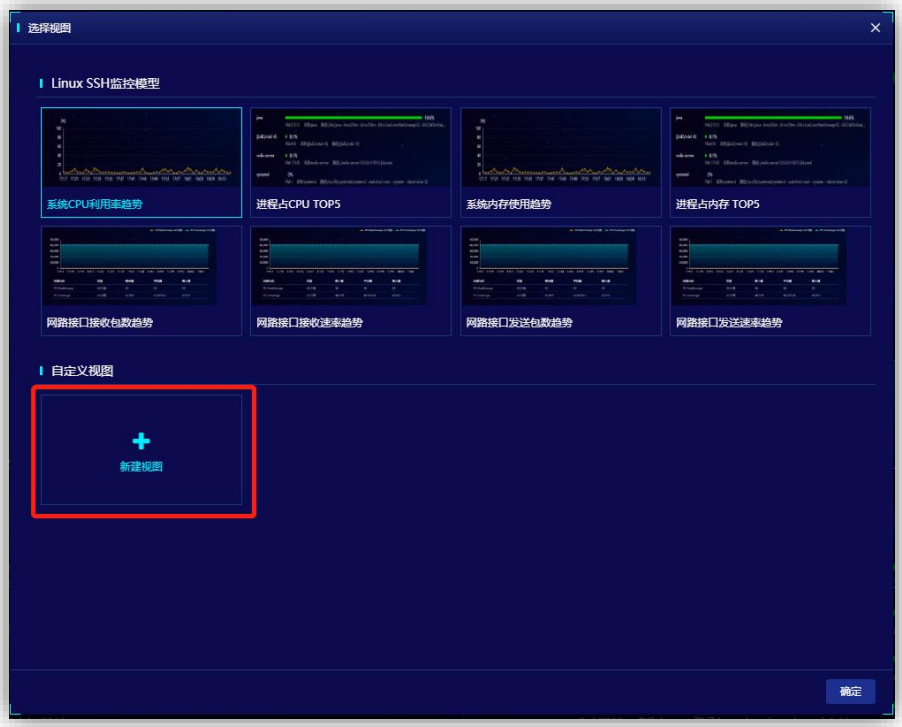


图 2-70 新建视图

- 输入视图名称并选择指标保存

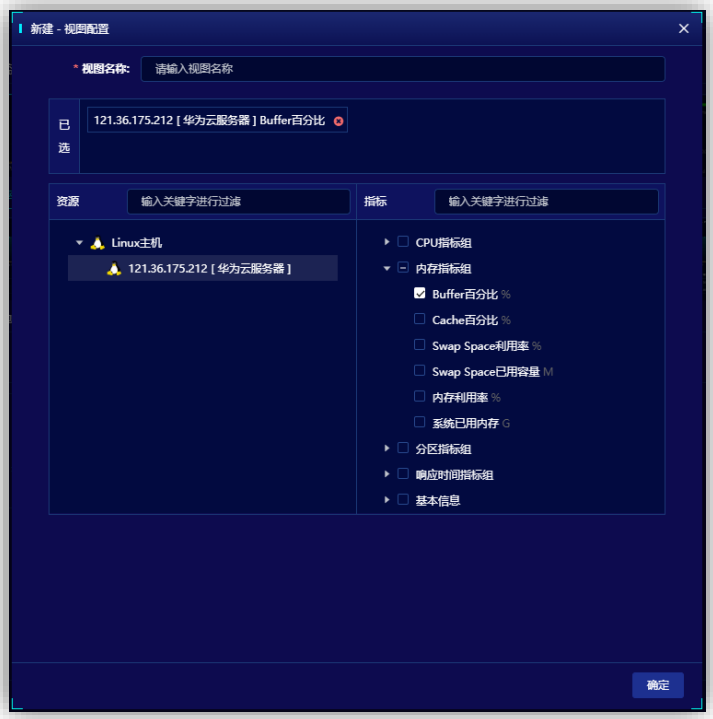


图 2-71 新建视图

2 业务应用创建

业务应用展示被监控业务系统的架构图。用户可自定义架构图、以拖拽画图形式描述系统软硬件关系。

2.1 创建业务应用

进入系统后点击业务应用菜单，点击窗口右下角的“+”图标在弹出的窗口中填写基本信息和模块信息。

图 3-1 业务应用菜单

2.1.1 填写基本信息

弹出的新建业务应用窗口中默认进入的是“基本信息”页签中，在窗口中填写应用名称、负责人、排序号等，以及请求信息（图中红色框部分），填写完成点击连接测试按钮，测试成功后弹出成功提示失败则弹出失败提示，成功后

点击确定按钮关闭窗口。

填写这部分信息时间，需要提前确定 URL 请求方式、URL 地址、请求参数等关键信息，这些信息如果不会填写请联系要监控的业务系统开发人员确定。

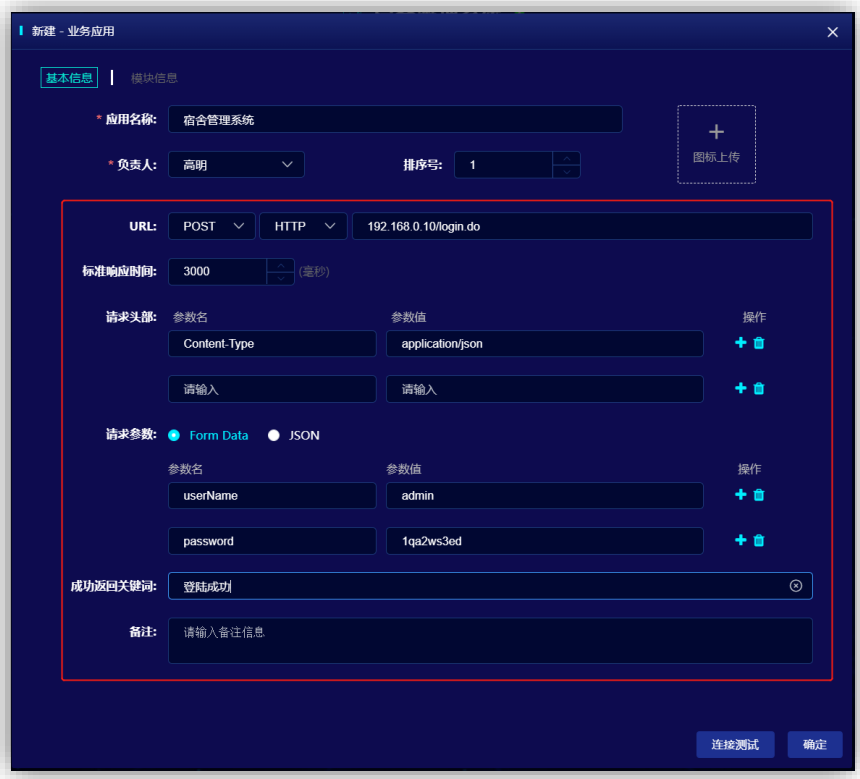


图 3-2 新建-业务应用

2.1.2 填写模块信息

如果想要监控业务系统中的模块信息时，可以在填写并保存完基本信息后，点击模块信息填写。填写规则与基本信息一致，唯一的区别是，模块信息是登录系统后的内部模块的请求地址与参数。

新建模块按照如下步骤进行。

- 点击编辑业务应用

图 3-3 编辑业务应用

- 点击模块信息

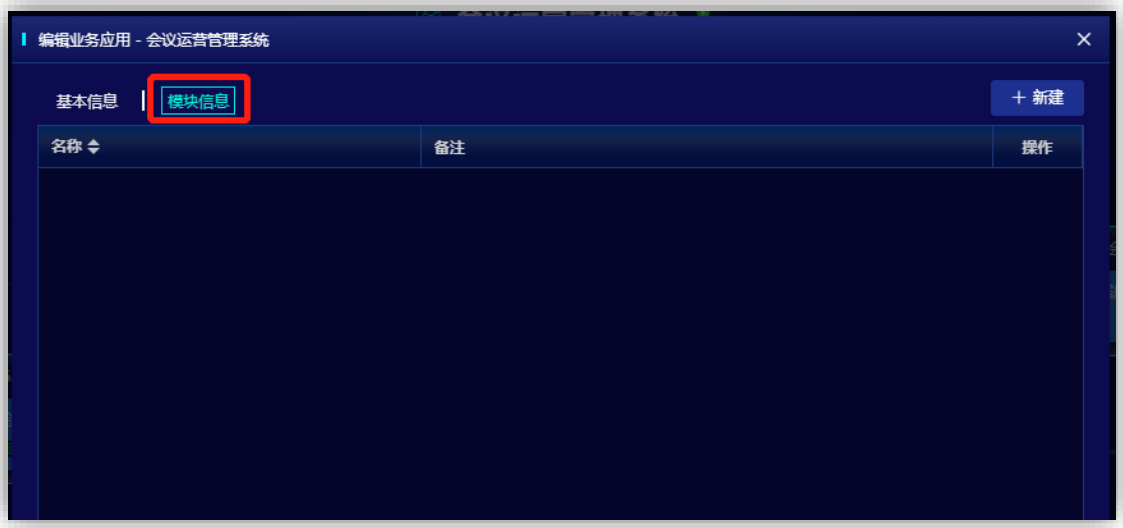


图 3-4 模块信息页面

- 点击新建按钮填写模块名称

图 3-5 新建模块信息

- 确定保存后点击名称编辑模块内容

图 3-6 编辑模块内容

2.2 编辑业务应用

鼠标移动到需要编辑的业务应用位置后，出现编辑按钮（图 3-3），点击编辑按钮打开窗口，编辑完成后点击确定。

2.3 删除业务应用

鼠标移动到需要删除的业务应用位置后，出现删除按钮(图 3-4)，点击删除按钮后，会立即删除业务应用及关联的架构图等资源。

2.4 创建架构图

架构图依托于业务应用，业务应用新建后即可以增加。

图 3-7 架构图

编辑架构图可以按照以下的步骤进行。

2.4.1 布局资源

- 点击右上方编辑按钮展开所有资源

图 3-8 架构图资源列表

- 鼠标左键点击某个资源后，拖拽到空白图上。
- 选择一种连线方式将两个资源连接到一起。

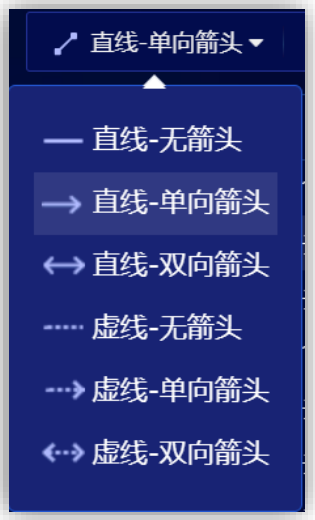


图 3-9 架构图中的资源连线方式

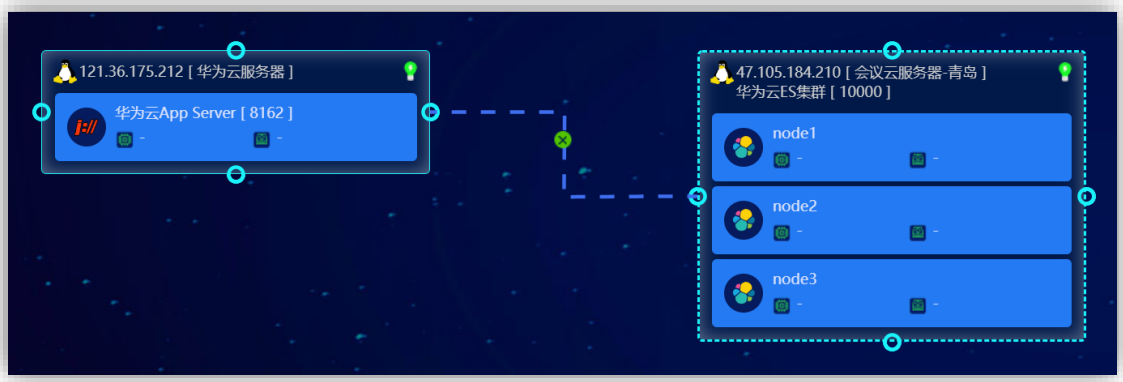


图 3-10 架构图中连接两个资源

2.4.2 选择监控指标

鼠标移动到监控资源上时，右侧会出现“齿轮”按钮(图 2-18)，点击后弹出选择监控指标窗口(图 2-19)，选择好监控指标后，点击确定后完成设置，该选中指标会被放置到监控资源上并显示当前值。

图 3-11 设置指标

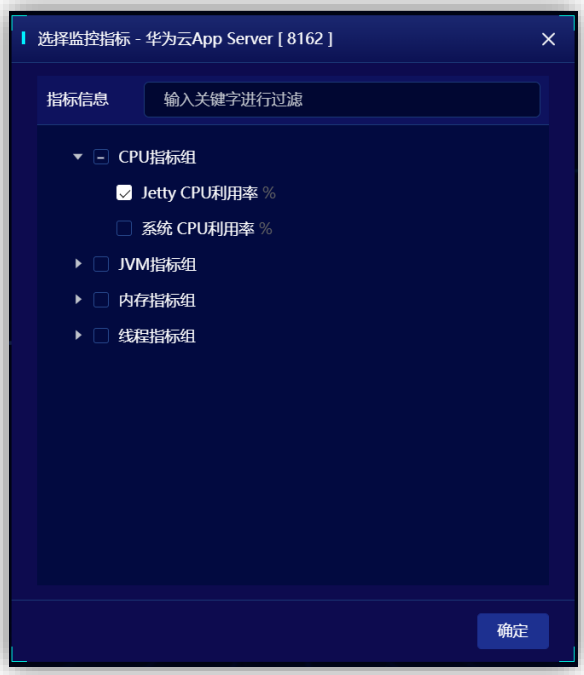


图 3-12 选择监控指标

2.4.3 添加关联指标

鼠标左键双击连线后，弹出添加关联指标窗口。从右侧窗口选择某一个指标，确定后该指标会显示到连线上。

图 3-13 添加关联指标

3 首页设置

3.1 初始化业务应用总览

- 系统安装后，点击首页新建业务应用总览，弹出首页设置窗口，选择业务应用总览布局后，点击下一步。

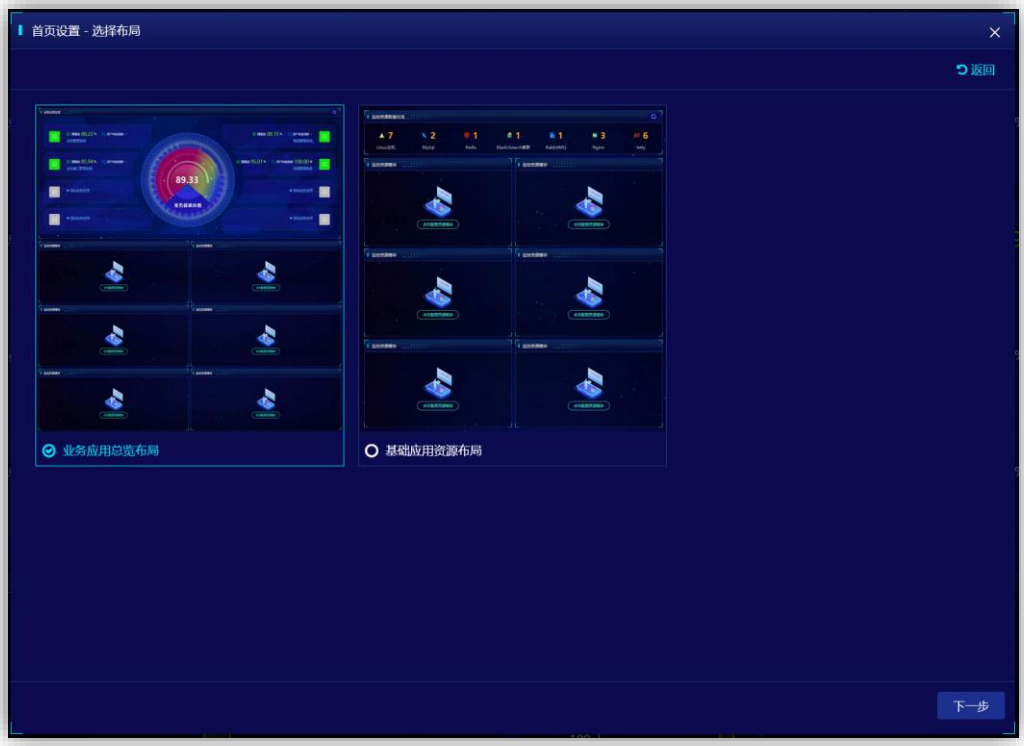


图 4-1 首页设置-选择布局

- 点击+按钮，再弹出的窗口中选择业务视图，点击确定。

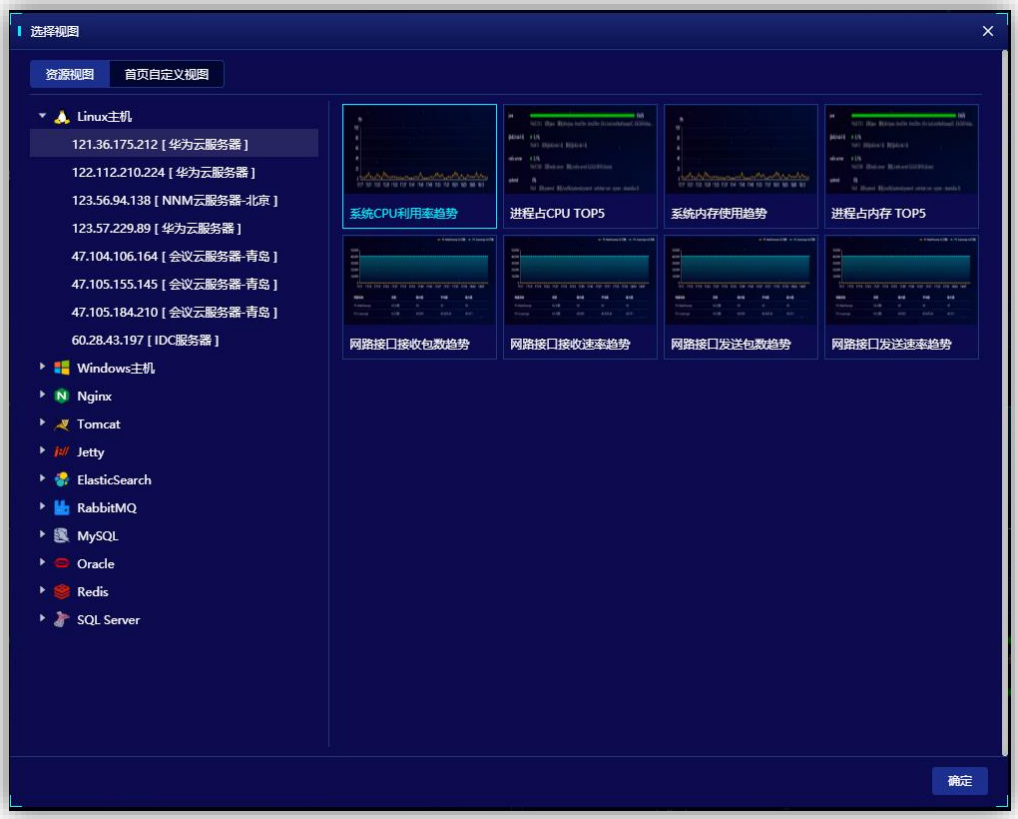


图 4-2 首页设置-配置 Portlet

3.2 添加业务应用

- 点击添加业务应用按钮

图 4-3 添加业务应用

- 从弹出的窗口中选择业务应用，点击确定

图 4-4 选择业务应用

3.3 调整资源模型视图

3.3.1 监控资源视图

- 在首页需要调整的资源视图工具条右上角处，点击编辑按钮

图 4-5 选择监控资源视图

- 选择模型视图，点击确定

图 4-6 选择视图

3.3.2 首页自定义视图

- 在选择视图窗口中点击首页自定义视图标签
- 点击新建按钮

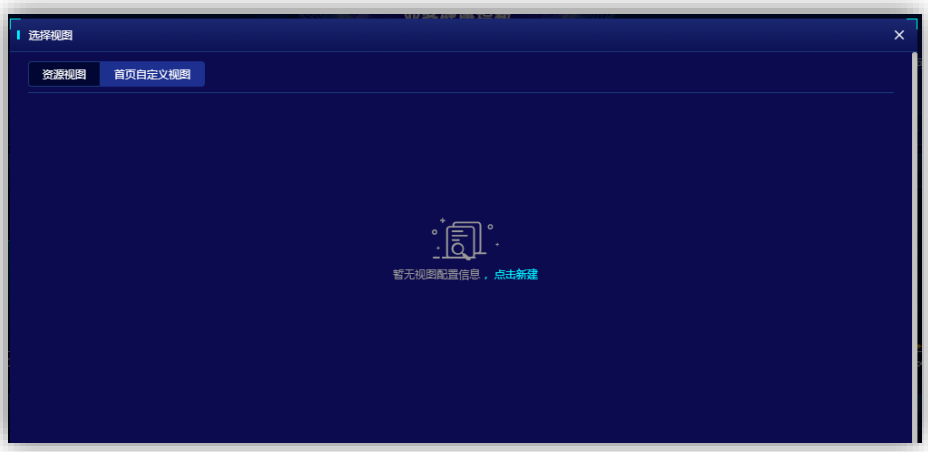


图 4-7 首页自定义视图

- 输入视图名称，选择指标后点击确定

图 4-8 新建视图配置

4 告警设置

4.1 资源告警配置

系统内置了资源默认的告警设置，也可针对被监控资源进行独立告警设置。下面以 Linux 服务器为例，详细说明如何配置。

- 进入资源管理，从资源列表中选择 Linux 服务器

图 5-1 资源管理页面

- 进入告警设置菜单

图 5-2 进入告警配置菜单

- 新建告警设置，告警设置可以设置告警条件（可多个条件组合）、添加

关联视图（告警信息出现后，可以看到关联的视图内容），输入标题后点击确定。告警类型可以选择可用性、性能、配置三种类型用于区分告警信息。

图 5-3 告警配置页面

图 5-4 新建告警配置页面

4.2 编辑资源告警配置

进入与资源告警配置相同的告警配置页面。可再右侧的表格中，编辑或删除设置过的告警配置。参见图 5-3。

5 消息通知设置

系统支持可用性告警、性能严重告警、全部告警信息的消息通知的推送。支持多种消息推送方式，可按照如下步骤进行设置。

进入系统后点击系统管理菜单、通知配置、消息通知配置，根据下图结合实际情况开启通知方式。可选的通知方式下面章节详细描述。

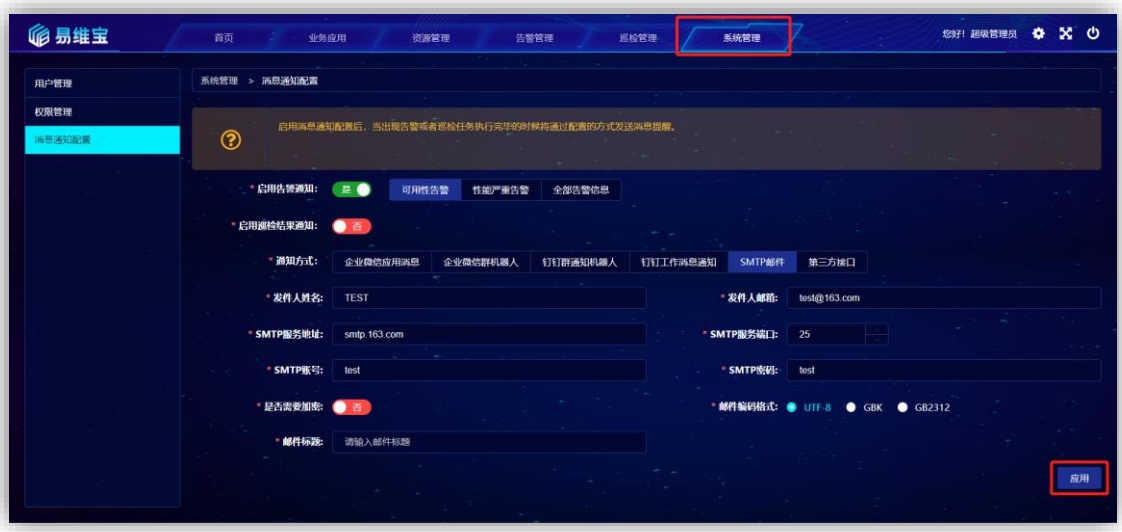


图 6-1 消息通知配置

5.1 企业微信应用消息设置

- 如何获取企业 ID、应用的凭证密钥、企业应用的 ID，请参考如下地址 https://blog.csdn.net/zxl782340680/article/details/79876502

5.2 企业微信群机器人设置

- 如何开启机器人并获取机器人 URL

https://jingyan.baidu.com/article/cbf0e500e4f46b6faa28938b.html

- 如何获取机器人 URL

Webhook 地址就是机器人 URL，从企业微信群里查看群机器人就可以看到

5.3 钉钉群通知机器人设置

- 如何开启机器人

https://jingyan.baidu.com/article/f0e83a25d748bf63e491015b.html

5.4 SMTP 邮件设置

可以使用邮箱的 SMTP 协议发送通知邮件，需要设置发件人邮箱的 SMTP。

- 发件人邮箱如何设置 SMTP，以网易邮箱为例，请参考如下链接。

https://jingyan.baidu.com/article/4e5b3e19266fee91901e2489.html

5.5 第三方接口设置

需要与第三方约定

6 账号权限管理

系统配置完成后，需要系统管理员分配账号并提供给运维人员。通过下面的步骤进行。

6.1 创建角色

- 进入系统后点击系统管理、权限管理

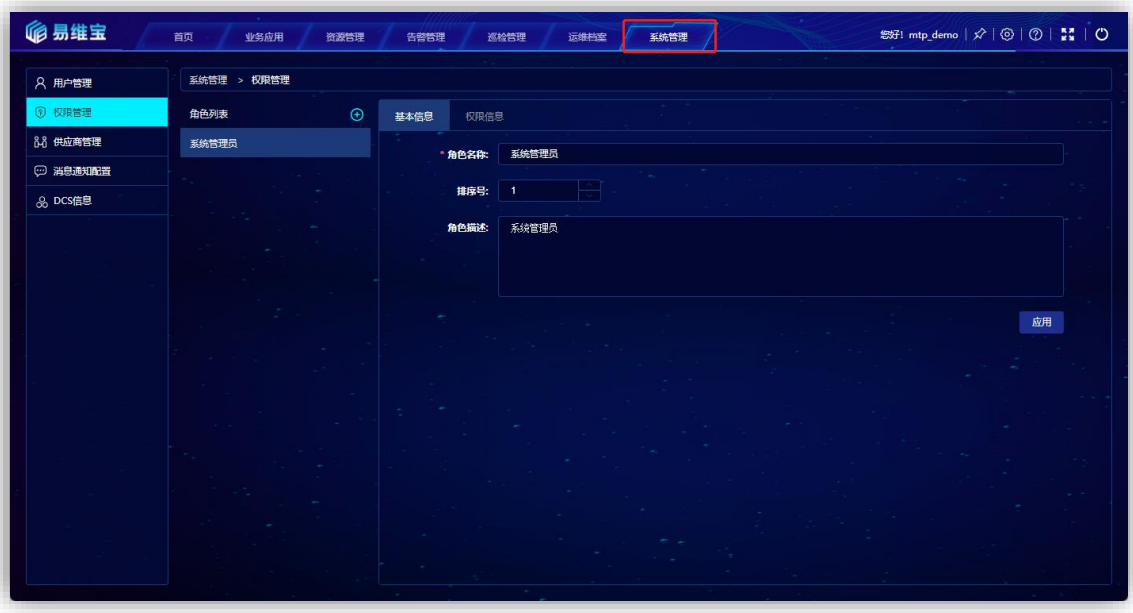


图 7-1 权限管理页面

- 进入系统后点击系统管理、权限管理、点击添加角色按钮

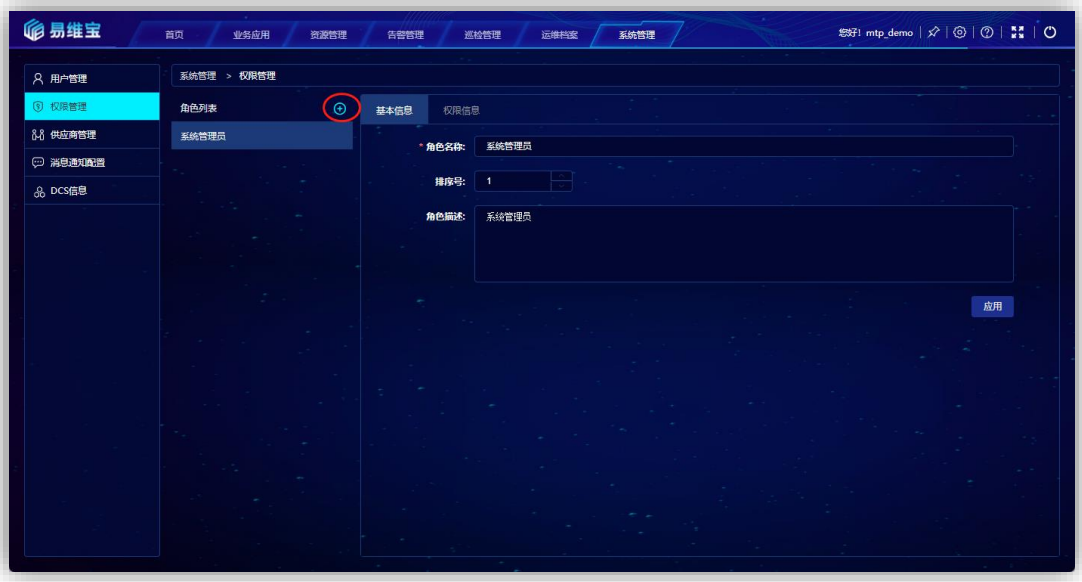


图 7-2 权限管理页面

- 输入基本信息后，点击应用

图 7-3 基本信息页面

- 点击角色列表中刚添加的角色后，选择权限信息后点击应用

图 7-4 权限信息分配

6.2 创建用户

- 进入系统后点击系统管理、用户管理，点击新建按钮

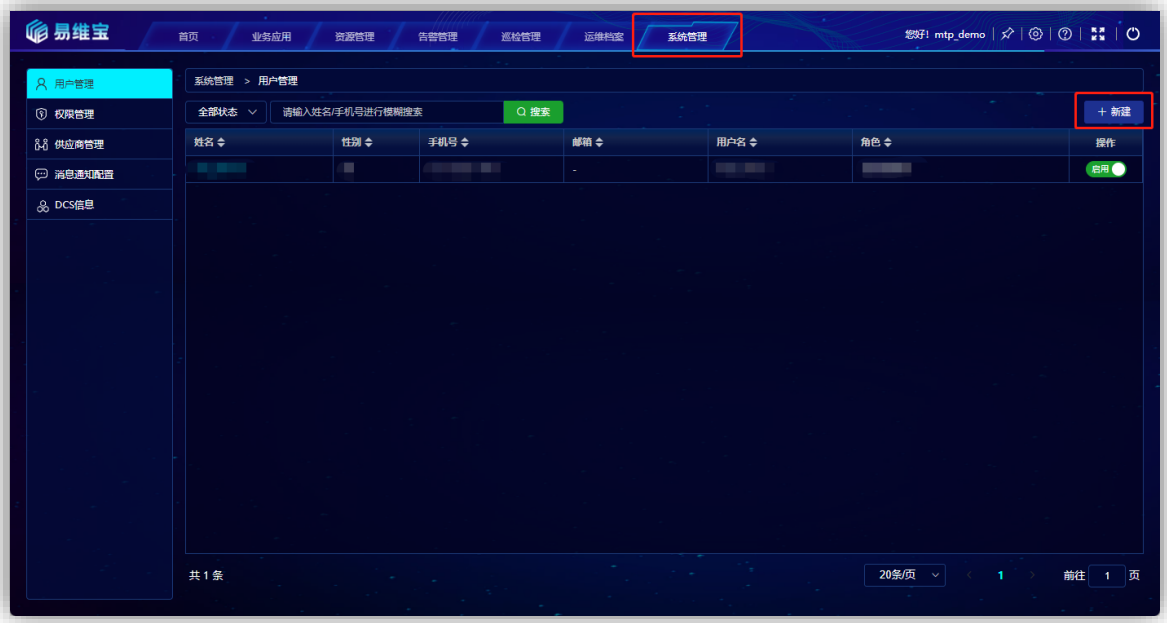


图 7-5 用户管理页面

- 输入用户信用信息后，选择角色后，点击确定，保存用户

图 7-6 输入用户信息

- 用户创建好以后，用新建的用户即可登录系统

7 运维档案

运维工程师编写并记录运行与维护记录形成运维档案，日常维护、安装部

署等等都可以记录，为日后查找问题和溯源时提供依据。每次编写的运维档案，如果选择了业务应用和基础资源，系统会自动建立关联关系，并在对应的业务应用和基础资源内显示。

图 8-1 运维档案