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…		4
	1.1	如	可下载 DCS	4
	1.2	如	可安装 DCS	4
1	发现	资源…		4
	1.1	主相	坈	5
		1.1.1	Linux 主机	5
		1.1.2	Windows 主机	9
	1.2	We	b Server	
		1.2.1	IIS	
		1.2.2	Apache	
		1.2.3	Nginx	
	1.3	Ap	plication Server	
		1.3.1	Jetty	
		1.3.2	Tomcat	
	1.4	中ì	间件	
		1.4.1	RabbitMQ 集群	
		1.4.2	ElasticSearch 集群	
	1.5	数	居库	
		1.5.1	SQLSERVER	
		1.5.2	GBase	
		1.5.3	达梦	74
		1.5.4	Redis	
		1.5.5	PostgreSQL	
		1.5.6	Oracle	
		1.5.7	MariaDB	
		1.5.8	MySQL	
	1.6	调	整资源模型视图	
		1.6.1	更换模型视图	
		1.6.2	自定义视图	
2	业务	应用创	健	
	2.1	创致	建业务应用	
		2.1.1	填写基本信息	
		2.1.2	填写模块信息	
	2.2	编	<u> </u>	110

	2.3	删降	除业务应用	111
	2.4	创建	建架构图	111
		2.4.1	布局资源	111
		2.4.2	选择监控指标	113
		2.4.3	添加关联指标	
3	首页	设置…		
	3.1	初如	始化业务应用总览	
	3.2	添加	加业务应用	
	3.3	调	整资源模型视图	
		3.3.1	监控资源视图	
		3.3.2	首页自定义视图	
4	告聲	设置		
	4.1	资	原告警配置	
	4.2	编	辑资源告警配置	
5	消息	通知设	置	
	5.1	企	业微信应用消息设置	
	5.2	企	业微信群机器人设置	
	5.3	钉	钉群通知机器人设置	
	5.4	SM	ITP 邮件设置	
	5.5	第	三方接口设置	
6	账号	权限管	理	
	6.1	创建	建角色	
	6.2	创建	建用户	
7	运维	档案…		

1 安装部署

1.1 如何下载 DCS

- 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

	_	9 .2 7			
Ŧ	tilada (†	B遠添加 全部編辑	Q、输入端口或者授权双	时象进行搜索	
	授权策略	优先级 〇	协议类型	端口范围 ①	授权对象①
	⊘ 允许	81	自定义 TCP	目的: 80/80	渡; 0.0.0.0/0
	② 允许	-1	自定义 TCP	目的: 50000/51000)厦: 0.0.0.0/0
	⊘ 允许	1	自定义 TCP	目的: 21/21	源: 0.0.0.0/0
	◎ 允许	1	自定义 TCP	目的: 10200/10230	源; 0.0.0.0/0
	◎ 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0
	② 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0

- 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

		业务应用 资源管理	告警管理 巡检管理 系统管理	総好! 超级管理员 🌩 Ů
资源	♀ 🟪 60.28.43.210 [IDC服务器-Win2012]	告警信息 (0)		♀ .15分钟 ▼
列表	Ⅰ 基本信息	8天9小时	最近7天可用性	
	○ 名称: 60.28.43.210	连续运行时间	09:18 09-19 09-20 09-21	09-22 09-23 09-24
	 新王名: 60.28.43.210 [IDC 艱珍書 Win201 操作系统版本: Windows Version 6.3 (Buil 	0 IEEE	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	参容量 39.66 GB ご用 32.78 GB
	▲ 系统CPU利用率趋势	4H • C @	■ 系统内存使用趋势	1H+ C @
		E 1650 1746 1740 1846 1940	(G) 4 3 2 1 0 2 2 1 0 2 2 1 0 2 2 1 2 1 2 1 2 1	◆ 系統部件 ◆ 系統已用以存 ● 系統部件 ● 系統已用以存

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

* 资源模型:	请选择			
	 O 主机	>	📒 Windows主机 🛛 >	O Linux SSH监控模型
	O Web Server	>	🙏 Linux主机 🔷 👌	O 麒麟Linux SSH监控模型
	O Application Server	>		
	○ 中间件	>		
	Ο 数据库	>		

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。

* 资源模型:	主机 / Linux主机 / Linux SSH监控模型			
	1、安装iostat命令(yum install iostat),如E	已经装过可以跳过		
	2、安装lsof命令(yum install lsof),如已经	责过可以跳过		
	3、安装python2.7,如已经装过可以跳过			
?	4、确认用户以上命令及tmp目录的操作权限			
* IP地址:	121.36.175.212	* SSH端口:	22 <u>^</u>	
* 用户名:	root	* 密码:	123456	

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

🖉 运行		×				
回 文作	ndows 将根据你所输入的名称,为你打开相应的 4夹、文档或 Internet 资源。	程序、				
打开(<u>O</u>): se	rvices.msc	~				
	确定 取消 浏览	ද <u>්(B</u>)				
9. 服务					-	
文件(E) 操作(A)	查看(V) 帮助(H)					
> + 	@ 🕞 🖥 📷 🕨 🔳 🕪					
) 服务(本地)	名称	描述	状态	启动类型	登录为	
	💁 System Guard 运行时监视器代理	监视	正在运行	目动(延迟启动, 触发器启动)	本地系统	
	System Events Broker	协调	正在运行	目动(触发器启动)	本地系统	
	System Event Notification Service	监视	正在运行	自动	本地系统	
	Q. SysMain	维护		手动	本地系统	
	SynTPEnh Caller Service		正在运行	自动	本地系统	
	🖏 SunloginService	Sunl		手动	本地系统	
	Storage Tiers Management	优化		手动	本地系统	
	Storage Service	为存	正在运行	目动(延迟启动, 触发器启动)	本地系统	
	Still Image Acquisition Events	启动		手动	本地系统	
	🖏 State Repository Service	为应	正在运行	手动	本地系统	
	SSDP Discovery	当发	正在运行	手动	本地服务	
	SQL Server VSS Writer	提供	正在运行	自动	本地系统	
	🖏 Spot Verifier	验证		手动(触发器启动)	本地系统	
	Software Protection	启用		目动(延迟启动, 触发器启动)	网络服务	
	🖏 SNMP 陷阱	接收		手动	本地服务	
	Q SNMP 服务	便简	正在运行	目动	本地系统	
	Smart Card Removal Policy	允许		手动	本地系统	
	Smart Card Device Enumeration Service	为给		手动(触发器启动)	本地系统	
	Smart Card	管理		手动(触发器启动)	本地服务	
	Shell Hardware Detection	为自	正在运行	自动	本地系统	
	Shared PC Account Manager	Man		禁用	本地系统	
	Server	支持	正在运行	目动(触发器启动)	本地系统	
	Sensor Service	一项		手动(触发器启动)	本地系统	
	Sensor Monitoring Service	监视		手动(触发器启动)	本地服务	
	Sensor Data Service	从各		手动(触发器启动)	本地系统	

2) 安装 SNMP 服务方法

具体操作方法请参考如下链接:

Sensor Data Service

\扩展 \标准/

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

0.000											_
5(H)											_
入站规则											
名称 ② CneNote for Windows 10 SMBDirect (WARP-In)上的文件相打印 ③ SNMP 建分(UDP In) SNMP 指規提發(UDP In) SNMP 指規提發(UDP In) SNMP 指規提發(UDP In) TPM 虚拟智能卡若理(DCOM-In) TPM 虚拟智能卡若理(TCP-In) TPM 虚拟智能卡若理(TCP-In) TPM 虚拟智能卡若理(TCP-In) TPM 虚拟智能卡若理(TCP-In) TPM 虚拟智能卡若理(TCP-In) TPM 虚拟智能卡若理(TCP-In) VisualSVN Distributed File System Se ③ VisualSVN Server (TCP-In)	組 OneNote for Windows 10 SMBDirect上的文件和打印 SNMP 起於 SNMP 配約 SNMP 配納 TPM 些以智能十管理 TPM 些以智能十管理 TPM 些以智能十管理 TPM 些以智能十管理 VisualSVN Distributed Fil VisualSVN Server	配置文件 域で考用 所有 <u>気</u> なの用 の用 の用 の用 成 域で 考明用、公用 域 域 を 考 の用 に の 用 、 の 用 、 が 有 の の の の の の の の の の の の の の の の の の	巴印 是 否 是 否 否 否 否 否 否 焉 是	盤 允允 ^允 允允允允允允允允允		恒序 任何 Syst %Sy %Sy %Sy %Sy %Sy %Sy C:\Pr C:\Pr C.\Pr	本任何 任何 任何 任何 任何 任何 任何 任何 任何 任何 任何 任何 任何 任	运程地址 任何 任何 年地子列 任何 本地子列 任何 本地子列 任何 年地子列 任何 年地子列 任何 任何 年 (一) (一) (一) (一) (一) (一) (一) (物议 任何 TCP UDP UDP UDP TCP TCP TCP TCP TCP TCP TCP TCP	本地調口 任何 5445 161 162 162 162 135 135 任何 任何 任何 任何	
 Wi-Fi Direct 后急处理程序使用体入) Wi-Fi Direct 扫描服务使用体入) Wi-Fi Direct 扫描服务使用体入) Wi-Fi Direct 网络发现体入) Windows Defender 防火地运程管理(凡, Windows Defender 防火地运程管理(凡, Windows Defender 防火地运程管理(R, Windows Defender 防火地运程管理(R, Windows Management Instrumentation) 	Wi-Fi Direct 网络发现 Wi-Fi Direct 网络发现 Wi-Fi Direct 网络发现 Windows Defender 称火 Windows Defender 称火 Windows Defender 称火 Windows Defender 称火 Windows Management In	公用 公用 公用 专用,公用 域 专用,公用 域 专用,公用	皇皇皇后百百百百	允许许许许许 并并并并并并并并	ka ka ka ka ka ka ka	%Sy %Sy %Sy %Sy %Sy %Sy %Sy	任何任任何有可可可	任何 任何 任何 本地子网 任何 本地子网 任何 本地子网	任何 任何 任P TCP TCP TCP TCP	任何 任何 RPC 助起 RPC 助起 RPC 烧线 RPC 烧线 任何	
	 (人社児気) (人社児気) (今日、日本日本の「の「い」」」、「の「い」」、「の「い」」、「の「い」」、「の「い」」、「の「い」」、「の「い」」、「の「い」」、「の「い」」、「の「い」、「の「い」、「の「い」、「の「い」、「の「い」、「の「い」、「の「い」、「の「い」、「の「い」、「の「い」、「、」、、、、、、、、、、						株式2000 相 配置文件 已用用 操作 智代 程序 合称 相 配置文件 已用用 操作 智代 程序 ② OneNote for Windows 10 CneNote for Windows 10 其 专用 星 允许 否 任何 ③ SNMD Eds (UDP In) SMBDirect 上的文件印印印。 SMMP Eds (UDP In) SMMP Eds (UDP In) <td> 株式の 人気化の 合称 福 配置文件 巳日用 単作 香代 昭子 本地地址 〇 OneNote for Windows 10 OneNote for Windows 10 MBDirect (WARP-In)上的文件印打印 SMBDirect 上的文件印打印 SMBDirect (WARP-In)上的文件印打印 SMBDirect 上的文件印印 SMBDirect (WARP-In)上的文件印打印 SMBDirect 上的文件印打印 SMBDirect (WARP-In)上的文件印打印 SMBDirect 上的文件印打印 SMBDirect (WARP-In)上的文件印打印 SMMP 認知 G SMMP 認知 SMMP 認知 第 SMMP 認知 SMMP 認知 第 SMMP 認知 SMMP 認知 SMMP 認知 第 SMMP 認知 SMMP 認知</td> <td> 株式の 本状の 本状の 日本 本状の 日本 日本</td> <td> 株式の 人気化の 合称 福 配置文件 日息用 塩作 器件 留件 電子 本地改社 近程均本 5MBDirect 上的文件和打印 5MMP NAP 医外 5MMP NAP NAP 医外 5MMP NAP 医外 5MMP NAP NAP NAP 医外 5MMP NAP NAP NAP NAP PAR PA 5MMP NAP NAP NAP PAR PAR PAR PAR PAR PAR PAR PAR PAR P</td> <td> 株式の 本状の 本状の 日本 大体の 日本 日本</td>	 株式の 人気化の 合称 福 配置文件 巳日用 単作 香代 昭子 本地地址 〇 OneNote for Windows 10 OneNote for Windows 10 MBDirect (WARP-In)上的文件印打印 SMBDirect 上的文件印打印 SMBDirect (WARP-In)上的文件印打印 SMBDirect 上的文件印印 SMBDirect (WARP-In)上的文件印打印 SMBDirect 上的文件印打印 SMBDirect (WARP-In)上的文件印打印 SMBDirect 上的文件印打印 SMBDirect (WARP-In)上的文件印打印 SMMP 認知 G SMMP 認知 SMMP 認知 第 SMMP 認知 SMMP 認知 第 SMMP 認知 SMMP 認知 SMMP 認知 第 SMMP 認知 SMMP 認知	 株式の 本状の 本状の 日本 本状の 日本 日本	 株式の 人気化の 合称 福 配置文件 日息用 塩作 器件 留件 電子 本地改社 近程均本 5MBDirect 上的文件和打印 5MMP NAP 医外 5MMP NAP NAP 医外 5MMP NAP 医外 5MMP NAP NAP NAP 医外 5MMP NAP NAP NAP NAP PAR PA 5MMP NAP NAP NAP PAR PAR PAR PAR PAR PAR PAR PAR PAR P	 株式の 本状の 本状の 日本 大体の 日本 日本

操作(A) 查看(V)	希 坦(H)											
2 🔟 🗟 🖬												
计算机 上的高级安全	Wine 出站规则											ā
。sa规则	名称	组 ^	配置文件	已启用	攝作	替代	程序	本地地址	远程地址	协议	本地調日	1
出站规则	SNMP 服务(UDP Out)	SNMP 副祭	专用,公用	悬	允许	香	%Sy	任何	本地子网	UDP	任何	ľ
接安全规则	SNMP 服务(UDP Out)	SNMP 题符	1	-	和許		96Sy	任何	任何	UDP	任何	
ERIC.	TPM 虚拟智能卡管理(TCP-Out)	TPM 虚拟智能卡管理	专用,公用	香	允许	香	%Sy	任何	本地子网	TCP	任何	ĺ
	TPM 虚拟智能卡管理(TCP-Out)	TPM 虚拟智能卡管理	城	否	允许	쥼	%Sy	任何	任何	TCP	任何	
	♥Wi-Fi Direct 后台处理程序使用(输出)	Wi-Fi Direct 网络发现	公用	是	允许	否	%Sy	任何	任何	任何	任何	
	Wi・Fi Direct 扫描服务使用(輸出)	Wi-Fi Direct 网络发现	公用	是	允许	否	%Sy	任何	任何	任何	任何	
	🕑 Wi-Fi Direct 网络发现(输出)	Wi-Fi Direct 网络发现	公用	最	允许	否	%Sy	任何	任何	任何	任何	
	Windows Defender SmartScreen	Windows Defender Smart	所有	是	允许	否	任何	任何	任何	任何	任何	
	Windows Feature Experience Pack	Windows Feature Experie	所有	是	允许	否	任何	任何	任何	任何	任何	
	Windows Management Instrumentati	Windows Management In	括	否	允许	否	%Sy	任何	任何	TCP	任何	
	Windows Management Instrumentati	Windows Management In	专用,公用	杏	允许	否	%Sy	任何	本地子网	TCP	任何	
	Windows Media Player (TCP-Out)	Windows Media Player	所有	否	允许	否	%Pr	任何	任何	TCP	任何	
	Windows Media Player (UDP-Out)	Windows Media Player	所有	否	允许	否	96Pr	任何	任何	UDP	任何	
	Windows Media Player x86 (TCP-Out)	Windows Media Player	所有	苦	允许	否	96Pr	任何	任何	TCP	任何	
	Windows Media Player x86 (UDP-Out)	Windows Media Player	所有	否	允许	否	%Pr	任何	任何	UDP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 网	专用,公用	否	允许	否	Syst	任何	本地子网	TCP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 阿	ᆀ	否	元许	否	Syst	任何	任何	TCP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 阿	胡	否	允许	否	%Sy	任何	任何	TCP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 阿	专用,公用	否	允许	否	%Sy	任何	本地子网	TCP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 网	ᆀ	否	允许	否	%Sy	任何	任何	UDP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 阿	专用,公用	否	允许	音	%Sy	任何	本地子网	UDP	任何	

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

入方向 出方向					
爭	315.110 (Hi	B 添加 全部编辑	Q、输入端口或者授权对象	进行搜索	
	授权策略	优先级 〇	协议类型	第口范围 ①	授权对象①
	② 允许	1	自定义 UDP	目的: 161/161	语: 0.0.0.0/0
3	②允许	1	自定义 TCP	目的: 10003/10004	源: 0.0.0.0/0
	②允许	1	自定义 TCP	目的: 4000/4000	源: 0.0.0.0/0
-	◎ 允许	1	全部	田台5: -1/-1	源: 10.137.42.136/24
	◎ 允许	1	全部	目的: -1/-1	源; 10.153.176.106/24
	◎ 允许	1	全部	目的: -1/-1	灋: 121.43.18.0/24
	②允许	ŧ	全部	目的: -1/-1	遷 120.55.177.0/24

- 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

常规 登录 ☑ 发送身份验 接受的社区	恢复 证陷阱(U	代理	陷阱	安全	依存关系	
☑ 发送身份验 接受的社区:	证陷阱(U				there a side	
接定的社区	(7 <i>6</i> -/61))				
社区	呂称(N)			权限		
public				只读		
1	添加(<u>D</u>)		编辑(Ð	删除(<u>R</u>)	
() 接受来!	自任何主制	LAD SNIN	AP 数据有	1(C)		
○ <u>1</u> <u></u> ○ <u></u> 接受来目	自下列主机	山 SNN	//P 数据包	1(T)		
-		-10 7.2		41		
	添加		编辑(])	删除(<u>M</u>)	

- 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

* 资源模型:	请选择			
	 O 主机		🛀 Windows主机 🔿	O Window SNMP监控模型
	O Web Server	>	🙏 Linux主机 💦 >	
	O Application Server	>		
	○ 中间件	>		
	Ο 数据库	>		

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。

1.安装SNMP服务 1) 控制面板打开或关闭Windows功能 2) 添加 SNMP服务	
1.安装SNMP服务 1) 控制面极打开或关闭Windows功能 2) 添加 SNMP服务	
1) 控制面板打开或关闭Windows功能 2) 添加 SNMP服务	
2) 添加 SNMP服务	
2.配置SNMP服务	
1) 添加接受的社区名称。设置团体权限	
2) 勾选发送身份验证陷阱	
3) 勾选接受来自任何主机的SNMP数据包(或添加允许的主机IP)	
4) 重启 SNMP服务	
* IP地址: 60.28.43.211 * 端口: 161 个	
* 只读共同体: public * 读写共同体: public	

- 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



9.服务					1	□ ×
文件(E) 操作(A)	查看(V) 帮助(H)					
🗢 🌩 💼 🖻	Q 🕞 🔣 📰 🕨 🔳 II II					
(3) 服务(本地)	名称	描述 状	态	启动类型	登录为	^
	🖏 System Guard 运行时监视器代理	监视 正	在运行	目动(延迟启动, 触发器启动)	本地系统	
	System Events Broker	协调 正	在运行	目动(触发器启动)	本地系统	
	System Event Notification Service	监视 正视	在运行	自动	本地系统	
	🖏 SysMain	维护		手动	本地系统	
	SynTPEnh Caller Service	E	在运行	自动	本地系统	
	🖏 SunloginService	Sunl		手动	本地系统	
	🖏 Storage Tiers Management	优化		手动	本地系统	
	🖏 Storage Service	为存 正	在运行	目动(延迟启动, 触发器启动)	本地系统	
	Still Image Acquisition Events	启动		手动	本地系统	
	State Repository Service	为应 正	在运行	手动	本地系统	
	SSDP Discovery	当发 正述	在运行	手动	本地服务	
	SQL Server VSS Writer	提供 正	在运行	自动	本地系统	
	Spot Verifier	验证		手动(触发器启动)	本地系统	
	Software Protection	启用		目动(延迟启动, 触发器启动)	网络服务	
	🖏 SNMP 陷阱	接收		手动	本地服务	
	SNMP 服务	便简 正	在运行	目动	本地系统	
	Smart Card Removal Policy	允许		手动	本地系统	
	Smart Card Device Enumeration Service	为给		手动(触发器启动)	本地系统	
	🖏 Smart Card	管理		手动(触发器启动)	本地服务	
	Shell Hardware Detection	为自 正	在运行	自动	本地系统	
	Shared PC Account Manager	Man		禁用	本地系统	
	🖏 Server	支持 正	在运行	目动(触发器启动)	本地系统	
	Sensor Service	—项		手动(触发器启动)	本地系统	
	Sensor Monitoring Service	监视		手动(触发器启动)	本地服务	
	Sensor Data Service	从各		手动(触发器启动)	本地系统	
	「「「」」、「「」」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」					

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

智能业务应用运维管理平台-用户使用手册

な件(E) 操作(A) 査看(V)	解助(円)										
• • 2 🔟 🗟 🖬	1										
本地计算机上的高级安全 W	fin: 入站规则										
123 入站规则	名称	细	配置文件	已启用	操作	暑代	程序	本地地址	远程地址	协议	本地調口
123 出站规则	OneNote for Windows 10	OneNote for Windows 10	城专用	星	允许	否	任何	任何	任何	任何	任何
连接安全规则	SMBDirect (iWARP-In)上的文件和打印	SMBDirect 上的文件和打印	所有	否	允许	香	Syst	任何	任何	TCP	5445
100 日間	SNMP 服务(UDP In)	SNMP 服务	坡		允许	香	%Sy	任何	任何	UDP	161
	SNMP 服务(UDP In)	SNMP 服务	今用,公用		允许		%Sy	任何	本地于网	UDP	
	SNMP 陷阱服务(UDP In)	SNMP 招請	城	否	允许	否	96Sy	任何	任何	UDP	162
	SNMP 陷阱服务(UDP In)	SNMP 阳研	专用,公用	否	允许	否	%Sy	任何	本地子网	UDP	162
	TPM 直拟智能卡管理(DCOM-In)	TPM 虚拟智能卡管理	专用,公用	否	ft#F	否	96Sy	任何	本地子网	TCP	135
	TPM 虚拟智能卡管理(DCOM-In)	TPM 虚拟智能卡管理	绒	否	抗汗	否	96Sy	任何	任何	TCP	135
	TPM 虚拟智能卡管理(TCP-In)	TPM 虚拟智能卡管理	城	否	允许	香	%Sy	任何	任何	TCP	任何
	TPM 虚拟智能卡管理(TCP-In)	TPM 透放聲能卡管理	专用,公用	否	允许	否	%Sy	任何	本地子网	TCP	任何
	VisualSVN Distributed File System Se	VisualSVN Distributed Fil	专用,公用	否	允许	否	C:\Pr	任何	本地子网	TCP	任何
	VisualSVN Distributed File System Se	VisualSVN Distributed Fil	城	否	允许	否	C:\Pr	任何	任何	TCP	任何
	VisualSVN Server (TCP-In)	VisualSVN Server	所有	鼎	允许	香	C:\Pr_	任何	任何	TCP	任何
	☑ Wi-Fi Direct 后台处理程序使用(输入)	Wi-Fi Direct 网络发现	公用	是	允许	否	96Sy	任何	任何	任何	任何
	Ø Wi-Fi Direct 扫描服务使用(输入)	Wi-Fi Direct 网络发现	公用	是	允许	否	%Sy	任何	任何	任何	任何
	Ø Wi-Fi Direct 网络发现(输入)	Wi-Fi Direct 网络发现	公用	是	允许	香	96Sy	任何	任何	任何	任何
	Windows Defender 訪火增近程管理(R	Windows Defender 15%-	专用,公用	否	抗汗	否	96Sy	任何	本地子网	TCP	RPC EDS
	Windows Defender 防火境远程管理(R	Windows Defender 100k	25	否	允许	否	%Sy	任何	任何	TCP	RPC EDE
	Windows Defender 防火境远程管理(R	Windows Defender 15%	专用,公用	否	允许	否	96Sy	任何	本地子网	TCP	RPC 终期
	Windows Defender 防火境远程管理(R	Windows Defender 防火	城	否	允许	香	%Sy	任何	任何	TCP	RPC 终期
	Windows Management Instrumentati	Windows Management In	专用公用	香	允许	쥼	96sy	任何	本地子网	TCP	任何

操作(A) 查看(V)	補助(土)											
2 🔟 🗟 🖬 🖬												_
计算机 上的巡视安全 V	fine 出站规则											
、站规则	名称	组 ^	配置文件	已启用	攝作	督代	程序	本地地址	远程地址	协议	本地調日	1
出站规则	SNMP 服务(UDP Out)	SNMP 副告	专用.公用	悬	允许	香	%Sy	任何	本地子网	UDP	任何	
1 接安全规则	SNMP 服务(UDP Out)	SNMP 副時	-	-	允许	畜	96Sy	任何	任何		任何	
宣視	TPM 虚拟智能卡管理(TCP-Out)	TPM 虚拟智能卡管理	专用,公用	香	允许	香	%Sy	任何	本地子网	TCP	任何	
	TPM 虚拟智能卡管理(TCP-Out)	TPM 虚拟智能卡管理	域	否	允许	좀	96Sy	任何	任何	TCP	任何	
	☑ Wi-Fi Direct 后台处理程序使用(输出)	Wi-Fi Direct 网络发现	公用	是	允许	香	%Sy	任何	任何	任何	任何	
	WivFi Direct 扫描服务使用(輸出)	Wi-Fi Direct 网络发现	公用	是	允许	否	%Sy	任何	任何	任何	任何	
	Wi-Fi Direct 网络发现(输出)	Wi-Fi Direct 网络发现	公用	是	允许	否	%Sy	任何	任何	任何	任何	
	Windows Defender SmartScreen	Windows Defender Smart	所有	是	允许	否	任何	任何	任何	任何	任何	
	Windows Feature Experience Pack	Windows Feature Experie	所有	是	允许	否	任何	任何	任何	任何	任何	
	Windows Management Instrumentati	Windows Management In	城	否	允许	香	%Sy	任何	任何	TCP	任何	
	Windows Management Instrumentati	Windows Management In	专用,公用	杏	允许	否	%Sy	任何	本地子网	TCP	任何	
	Windows Media Player (TCP-Out)	Windows Media Player	所有	否	允许	否	96Pr	任何	任何	TCP	任何	
	Windows Media Player (UDP-Out)	Windows Media Player	所有	否	允许	否	96Pr	任何	任何	UDP	任何	
	Windows Media Player x86 (TCP-Out)	Windows Media Player	所有	否	允许	否	96Pr	任何	任何	TCP	任何	
	Windows Media Player x86 (UDP-Out)	Windows Media Player	所有	杳	允许	否	96Pr	任何	任何	UDP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 网	专用,公用	否	允许	否	Syst	任何	本地子网	TCP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 阿	垣	否	元许	否	Syst	任何	任何	TCP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 阿	ᆀ	否	允许	否	%Sy	任何	任何	TCP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 阿	专用,公用	否	允许	쥼	%Sy	任何	本地子网	TCP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 网	披	否	允许	쥼	96Sy	任何	任何	UDP	任何	
	Windows Media Player 网络共享服务(Windows Media Player 阿	专用,公用	否	允许	否	96Sy	任何	本地子网	UDP	任何	

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

λ.	方向出方向	0			
爭	315.110 (Hi	B 添加 全部编辑	Q、输入端口或者授权对象	进行搜索	
	授权策略	优先级 〇	协议类型	第口范围 ①	授权对象①
	② 允许	1	自定义 UDP	目的: 161/161	语: 0.0.0.0/0
3	②允许	1	自定义 TCP	目的: 10003/10004	源: 0.0.0.0/0
	②允许	1	自定义 TCP	目的: 4000/4000	源: 0.0.0.0/0
-	◎ 允许	1	全部	田台5: -1/-1	源: 10.137.42.136/24
	◎ 允许	1	全部	目的: -1/-1	源; 10.153.176.106/24
	◎ 允许	1	全部	目的: -1/-1	源: 121.43.18.0/24
	②允许	ŧ	全部	目的: -1/-1	遷 120.55.177.0/24

- 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

服务 的属	性(本地社	 算机)				×
登录	恢复	代理	陷阱	安全	依存关系	
22 白八花	STROPH (0				
		9				
社区	≏孙(<u>11</u>)			权限		
public				只读		
E						1
	添加(D)	s	编辑(E)	删除(<u>R</u>)	_
)接受李	自任何主相	Πάς SNN	MP 数据的	1(C)		
) 接受来	自下列主机	几的 SNN	VP 数据的	1(T)		
						-
				-		
	契务的属 登录 送身份验 受的社区 加助目に) 接受未!	 	我务 的居住(本地計算机) 登录 恢复 代理 送身份验证陷阱(U) 受的社区名称(N) 社区 public 添加(D)… 援受未自任何主机的 SNM 送受未自下列主机的 SNM	R务 的属性(本地计算机) 登录 恢复 代理 陷阱 送身份验证陷阱(U) 受的社区名称(N) 社区 public 添加(D)… 编辑(编辑(读数学来自任何主机的 SNMP 数据 按要来自下列主机的 SNMP 数据	服务 的属性(本地计算机) 登录 恢复 代理 陷阱 安全 送身份验证陷阱(U) 受的社区名称(N) 社区 权限 public 只读 漆加(D) 编辑(E) 沙接受未自任何主机的 SNMP 数据包(C) 決要支援	服务 的属性(本地计算机) 登录 恢复 代理 陷阱 安全 依存关系 送身份验证陷阱(U) 受的社区名称(N) 社区 权限 public 只读 添加(D) 编辑(E) 搬除(B) 没要未自任何主机的 SNMP 数据包(C) 没要未自下列主机的 SNMP 数据包(D)

- 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

* 资源模型:	请选择	^			
	○ 主机	>	🍗 IIS		OⅡS V6.0及以上版本监控模型
	O Web Server		🝆 Apache	>	
	O Application Server	>	🔊 Nginx	>	
	○ 中间件	>			
	O 数据库	>			

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。

▲ 资源发现				×
* 资源模型:	Web Server / IIS / IIS V6.0及以上版本监控模型	<u>U</u>	~ ?	
* IP地址:	请输入IP地址	* 端口:	161 <u>^</u>	
* 只读共同体:	public	* 读写共同体:	public	
				发现

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

				1500
				12778
赵本岳思	最近7天可用性			
O 名称: 60.28.43.210			10-25 10-26	10-27
◎ 备注名: 115 8.0 [161] 🖉				
O IP地址: 60.28.43.210 ○ 旅校編目: 161	1 × × × × ×			
○ 当前连接许可证数: 0 个			0个 0	个
O 当前SSL连接的许可证数:0个	🧜 . 99% 🏏 0% 🦭	". 0% ". ". 0% "."	当前连续故 與3	国济求数
O I/O潭電分辨平均值: 0 byte	系统CPU利用率 IIS CPU利用率	系统内存利用率 IIS内存利用率		
		1 连接统计		
	→ 每时接收字节数 → 每时发送字节数		每秒尝试生物数	
(kb/sec) 1		- 1		
0 05:40 05:55 06:10 06:25 06:40 06:55 07:10 07:25 07:40 0	-55 08:10 08:25 08:40 08:55 09:10 09:25	0 05:40 05:55 06:10 06:25 06:40 06:55 0	7:10 07:25 07:40 07:55 08:10 08:25 08:40 08:55 0	9:10 09:25
1047-54911	48+ 0 0			4H • 1 Ω
	与时间日请求数 与时期间请求数 与时期日請次数		当的主服名法地用户服	
(^/B)		(1)		

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_<="" th=""><th>_config_module></th></ifmodule>	_config_module>
LogFormat	"{"ip":"%a","time":"%{ms}T","path":"%r","status":"%>s","bytes":"%b"}"
monitor	
CustomLog "lo	gs/monitor_access.log" monitor

- 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



● 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:\Use	rs\wang	qi>netsh fir	ewall show p	portopenir	ng
域 配計 端口	置文件的 协议	端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP	肩肩肩肩肩肩肩肩上	达达达达达达达达达		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 酉 端口	记置文件 协议	的端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩上	入入入入入入入入入入入入		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)。

Λ.	方向世	访问				
Ŧ	动添加	快速添加全部编辑	Q、 输入端口或者授权	対象进行搜索		
	授权策略	优先级 〇	协议类型	講□范围 ①	授权对象①	
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0.0/0	
	◎ 允许	-1)	自定义 TCP	目的: 50000/51000	源: 0.0.0/0	
	⊘ 允许	91.)	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
	(2) 允许	110	自定义 TCP	目的: 3369/3389	源: 0.0.0.0/0	

- 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

 ● 主机 > ● IIS > ● Apache V2.x及以上版 ● Application Server > ● 中间件 > ● 数据库 > > >	* 资源模型:	请选择 ^				
 ○ Web Server > ○ Application Server > ○ 中间件 > ○ 数据库 > 		▲ O 主机		🍗 IIS		● Apache V2.x及以上版:
 ○ Application Server > Nginx > ○ 中间件 > ○ 数据库 > 		O Web Server		👟 Apache		
 ○中间件 > ○数据库 > 		O Application Server		🐧 Nginx		
○ 数据库 >		○ 中间件				
		● 数据库				

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。

* 资源模型:	Web Server / Apache / A	Apache V2.x及以上	版本	~ ?	
O Apache连接信	息				
* IP地址:	请输入IP地址		* 端口:		
) 主机连接信息					
* 主机模型:	Linux主机		* 监控协议:	SSH协议	
* IP地址:	请输入IP地址		* 端口:	22 ×	
* 用户名:	请输入用户名		* 密码:	请输入密码	

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





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-strea	am;					
log_format	monitor	'{"ip":"\$remote_addr","time":				
ime","path":"\$request","status":"\$status","bytes":"\$bytes_sent"}';access_log						
/tmp/logs/monitor_access.log mon	itor;					
}						

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/nginxsbin-path=/usr/sbin/nginx	modules-
path=/usr/lib64/nginx/modulesconf-path=/etc/nginx/nginx.conf	error-log-
path=/var/log/nginx/error.loghttp-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;

}

3

● 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:\Use	rs\wang	qi>netsh fir	ewall show po	ortopenir	ng
域 配計 端口	置文件的 协议	端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩	—————————————————————————————————————		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 酉 端口	记置文件 协议	的端口配置: 流量方向	÷	名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩	入入入入入入入入入入入入入入		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)。

7	方向世	访问				
Ŧ	动添加	快速添加全部编辑	Q、 输入满口或者授权	対象进行撞索		
	授权策略	优先级 〇	协议类型	講□范围 ①	授权对象①	
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0.0/0	
	◎ 允许	×1.	自定义 TCP	目的: 50000/51000	源: 0.0.0/0	
	⊘ 允许	8 1 .)	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
	(2) 允许	110	自定义 TCP	目的: 3369/3389	源: 0.0.0.0/0	

- 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

* 资源模型:	请选择 ^					
	▲ O 主机		🍗 IIS		O Nginx V1.16及以上版a	
	O Web Server		👟 Apache			
	• Application Server		🔊 Nginx			
	○ 中间件					
	○ 数据库					

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。

*资源模型:	Web Server / Nginx / Nginx V1.16及以上版本		~ (?)
 Nginx连接信 	e.		
* IP地址:	请输入IP地址	* 端口:	
○ 主机连接信息			
* 主机模型:	Linux主机	* 监控协议:	SSH协议 ~
* IP地址:	请输入IP地址	* 端口:	22
* 用户名:	请输入用户名	* 密码:	请输入密码



● 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

Lava 监视和管理控制台 - controlRole@123.56.94.138:50400			×
▲ 连接(C) 窗口(W) 帮助(H)	4 11s	e i	×
概览 内存 线程 类 Ⅷ 概要 MBean			-
<pre>#XZ 1917 3XE 英 10 使我美 morent JMImplementation</pre>			

- 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

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:\Use	ers\wang	gqi>netsh fi	rewall sho	w portopenin		
C:\Use	ers∖wang	qi>netsh fir	ewall show	portopening		
域 配) 端口	置文件的 协议	端口配置: 流量方向		名称		
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩	动站站站站站站站站站 站		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC	OL_UDP_8879_in OL_UDP_8878_in OL_UDP_21346_in OL_UDP_68_in OL_UDP_67_in OL_UDP_67_in OL_TCP_21735_in OL_TCP_9876_in OL_TCP_31637_in
标准 [端口	配置文件 协议	的端口配置: 流量方向		名称		
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP		 		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC zapya_NET_FW_IP_PROTOC	0L_UDP_8879_in 0L_UDP_8878_in 0L_UDP_21346_in 0L_UDP_68_in 0L_UDP_67_in 0L_TCP_21735_in 0L_TCP_9876_in 0L_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)

Ŧ	动添加 快	遠添加 全部編集	Q 输入端口或者授权3	对象进行搜索		
	授权策略	优先级 〇	协议类型	端口范围 ①	授权对象①	
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0.0/0	
	②允许	1	自定义 TCP	目的: 50000/51000	源: 0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	② 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
Π	② 允许	110	自定义 TCP	目的: 3369/3389	源: 0.0.0.0/0	

- 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

* 资源模型:	请选择			
	 ● 主机 	j:// Jetty		O Jetty V9.x及以上版本
	O Web Server	減 Tomcat	>	
	O Application Server			
	○ 中间件			
	Ο 数据库			

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。

*资源模型:	Application Server / Jett	ty / Jetty V9.x及以	L版本	~ (?)	
O Jetty连接信息					
* IP地址:	请输入IP地址		* 端口:		
用户名:	请输入用户名		密码:	请输入密码	
○ 主机连接信息					
* 主机模型:	Linux主机		* 监控协议:	SSH协议	
* IP地址:	请输入IP地址		* 端口:	22 <u>^</u>	
* 用户名:	请输入用户名		* 密码:	请输入密码	

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

内存 线程 类 Wit 概要 Millean		
Catalina	属性值	
Connector	名称	值
8009	URIEncoding	HTE-S
出現在	accentCount	100
世 課作	address	
田 <u></u> 通知	aipFlush	true
n 1	allowTrace	false
Deployer	ciphers	
7 Engine	ciphersUsed	
Rilter	className	
Clabel Person Processor	connectionLinger	-1
Vert	connectionTimeout	-1
TraManitar	enableLookups	false
Lander	executorName	Internal
MeanFactory	keepAliveTimeout	-1
Monagar	localPort	8009
Mannar	maxHeaderCount	100
ManingResources	maxKeepAliveRequests	
ParallalEahannClassInadar	maxParameterCount	10000
ProtocolHandlar	maxPostSize	2097152
Realm	maxSavePostSize	4096
Resource	maxSwallowSize	
Server	maxThreads	200
B Service	minSpareThreads	10
Servlet	modelerType	
M StringCache	packetSize	8192
ThreadPool	port	8009
Valve	processorCache	200
WebModul e	protocol	AJP/1.3
WebResourceRoot	protocolHandlerClassName	org. apache. coyote. ajp. AjpNioProtocol
Mimplementation	proxyName	
Users	proxyPort	0
com. sun. management	redirectPort	8443
java lang	scheme	http
java nio	secret	
java. util. logging	secure	false
a	sslProtocols	

- 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:\Use	rs\wang	qi>netsh fir	ewall show porto	ppening
域 配計 端口	置文件的 协议	端口配置: 流量方向	名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	启启启启启启启启启启启	入入入入入入入入入入入入	Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准西端口	记置文件 协议	的端口配置: 流量方向	名称	κ.
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩上的	入入 站站站站站站站站站站站站	Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)

У	方向出力	方向			
Ŧ	动添加	快速添加全部编辑	Q、输入端口或者授权对象进行搜索		
	授权策略	优先级 〇	协议类型	端口范围 ①	授权对象 ①
	⊘ 允许	3 1	自定义 TCP	目的: 80/80	渡; 0.0.0/0
	② 允许	4	自定义 TCP	目的: 50000/51000	源: 0.0.0/0
	⊘ 允许	1	自定义 TCP	目的: 21/21	源: 0.0.0/0
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0
	② 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0/0
	(2) 允许	110	自定义 TCP	目的: 3389/3389	源: 0.0.0.0/0

- 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

资源发现					×
* 资源模型:	□请选择 ^				
	● ● 主机	>	j:// Jetty	>	O Tomcat v8.x及以上版本
	O Web Server	>	🗶 Tomcat		
	O Application Server				
	○ 中间件	>			
	O 数据库	>			
					发现

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。

"资源快型:	Application Server / Tomc	at / Tomcat v8.x及以上版本			
O Tomcat连接信	息				
* IP地址:	请输入IP地址		* 端口:		
用户名:	请输入用户名		密码:	请输入密码	
○ 主机连接信息					
* 主机模型:	Linux圭机	× •1	拉拉协议 :	SSH协议	
* IP地址:	请输入IP地址		* 端口:	22 A	
* 用户名:	请输入用户名		* 密码:	请输入密码	

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

偷 易维宝 前 3/4	业务应用 资源管理 告	警管理 巡检管理 系统管理	悠好!系統管理员 🌣 🔀 😃
资 💡 👷 华为云App Server [8163] 连接器(1) 👻	应用(1) → 告聲信息 (0)		℃ 15分钟 - ◎ - ◎ -
列 王	③ 288 来 22 小时 连续运行时间	(2) 総行天可用性 10-21 10-22 10-23 10-24	10-25 10-26 10-27
 ○ 版本: 90.170 ○ PID: 31284 ○ 安装目录: /tmp/tomcat.12356838539361698 ○ JVM版本: Oracle Corporation / 1.8 ○ 提作系表: Linux / amd64 / 3100-1062.1.1.el 		к. к. к. к. к. к. к. к. к. к.	総容置 0.0 M 已用 0.00 M 交換空间(0%)
连接器线程总缆	0.1	I JVM CPU利用率	1H - C
200 Max Threads 10 Min spare threads http-mid	Current Threads 10 Busy Thread 0	(%) 100 80 40 20 0 0 0 0 0 0 0 0 0 0 0 0 0	
		09:30 09:35 09:40 09:45 09:50 09:55 10:4	

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:\Use	rs∖wang	qi>netsh fir	ewall show porto	pening
域 配置 端口	置文件的 协议	端口配置: 流量方向	名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP TCP TCP TCP	 	入入入入入入入入入入入入	Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 曹 端口	記重文件 协议	的端口配置: 流量方向	名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩上的	入入	Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)

λ	方向出	方向			
Ŧ	动态加	快速添加全部编辑	Q、输入端口或者授权对象进行搜索		
	授权策略	优先级 〇	协议类型	端口范围 ①	授权对象 ①
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0.0/0
	② 允许	а <u>т</u>	自定义 TCP	目的: 50000/51000	源; 0.0.0 .0/0
	⊘ 允许	1	自定义 TCP	目的: 21/21	源: 0.0.0.0/0
	⊘ 允许	<u>ч</u>	自定义 TCP	目的: 10200/10230	·源: 0.0.0.0/0
	② 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0/0
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0/0
	(2) 允许	110	自定义 TCP	目的: 3389/3389)便: 0.0.0.0/0

- 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

资源发现				×
* 资源模型:	请选择			
	▲ O 主机	📙 RabbitMQ	>	○ RabbitMQ集群-v3.8及以上版本
	O Web Server	😵 ElasticSearch	>	
	O Application Server			
	O 中间件			
	Ο 数据库			
				发现

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。

▶ 资源发现				×
* 资源模型:	中间件 / RabbitMQ / RabbitMQ集群-v3.8及以	上版本	× ?	
* IP地址:	请输入IP地址	* 靖口:		
* 用户名:	请输入用户名	* 密码:	请输入密码	
				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

💡 🔚 华为云Rab	bitMQ [10005]		告警信息 (1)							0 1599 4 (0)	
1 200768C1			9	381	22.2	381	*	最近7天可用性			
protocol	Node	Bound to	Port	版本	Erlang版本	插件管理版本	统计信息开关	10-21 10-22	10-23 10-24	10-25 10-26	10-2
amqp	rabbit@node2		10004								
amqp	rabbit@node3		10004	1 关键指标信息							
clustering	rabbit@node1		25672								
clustering	rabbit@node2		25672	3	10	10	j 10	Į 5	į 1	1-0	
clustering	rabbit@node3		25672	Node数量	许接数量	通道数量	Exchange数量	Query数量	Vhost数量	消费者数量	
http	rabbit@node2		10005								
Context	node	Port	path -							- Ready UnCheck	
RabbitMQ Manag	rabbit@node2	10005	/	500							
RabbitMQ Manag ement	rabbit@node3	10005		400							
RabbitMQ Promet heus	rabbit@node2	15692		- 200							
RabbitMQ Promet heus	rabbit@node3	15692		0 06:30 0	06:45 07:00 07:	15 07:30 07:45	08:00 08:15 08:30	08:45 09:00	09:15 09:30 (09:45 10:00 10:	15
消息处理速率										48 • 0	

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:\Use	rs∖wang	qi>netsh fir	ewall show po	ortopenin	g
域 配置 端口	置文件的 协议	端口配置: 流量方向	÷	名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩上	—————————————————————————————————————		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 曹 端口	记置文件 协议	的端口配置: 流量方向	Ĥ	名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP		——————————————————————————————————————		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)

Λ.	方向世	访问				
Ŧ	动添加	快速添加全部编辑	Q、 输入端口或者授权	対象进行搜索		
	授权策略	优先级 〇	协议类型	講□范围 ①	授权对象①	
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0.0/0	
	◎ 允许	-1)	自定义 TCP	目的: 50000/51000	源: 0.0.0/0	
	⊘ 允许	91.)	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
	(2) 允许	110	自定义 TCP	目的: 3369/3389	源: 0.0.0.0/0	

- 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

● 主机 > LasticSearch集群监控模型 ● 建机 > 像 ElasticSearch > ● Application Server > ● 中间件 > ● 数据库 >	*资源模型:	请选择			
 ○ Web Server > ○ Application Server > ○ 中间件 > ○ 数据库 > 		▲ O 主机	>	RabbitMO >	O ElasticSearch集群监控模型
O Application Server > O 中间件 > O 数据库 >		O Web Server	>	ElasticSearch >	
 ○ 中间件 > ○ 数据库 > 		O Application Server	>		
O 数据库 >		O 中间件			
		○ 数据库	>		

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 年 府 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

■ 服务器属性 - 192.168.1.104	,1433\MSSQLSERVER01		3276		×
选择页	🗊 脚本 🔻 🕝 帮助				
 内存	 服务器身份验证 ♥ Windows 身份验证模式(型) ● SQL Server 和 Windows 身份 登录审核 ○ 无(図) ● 仅限失败的登录(E) ○ 仅限成功的登录(E) ○ 失败和成功的登录(E) 	检证模式(<u>S</u>)			
连接	服务器代理帐户 ————————————————————————————————————				
服务器: 192.168.1.104,1433\MSSQLSER 注接: DESKTOP-GII39VQ\fujie ♥ 查看注接属性	□ 月用加研設部(12年10/10) 代理帐户(限): 密码(D): 法项 □ 符合通用标准符合性(0) □ 启用 C2 审核跟踪(E) □ 跨数据库所有权链接(C)				
进度					
就绪					
			确定	取	消

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:\Use 域配 端口	rs\wang 置文件的 协议	gi>netsh fir 端口配置: 流量方向	ewall show	portopenir 名称	lg
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩	· 入入入入入入入入入入入		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 酉 端口	2置文件 协议	的端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	 肩肩肩肩肩肩肩肩肩上。 	入入入入入入入入入入入入入入		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)

Λ.	方向世	访问				
Ŧ	动添加	快速添加全部编辑	Q、 输入端口或者授权	対象进行搜索		
	授权策略	优先级 〇	协议类型	講□范围 ①	授权对象①	
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0.0/0	
	◎ 允许	-1)	自定义 TCP	目的: 50000/51000	源: 0.0.0/0	
	⊘ 允许	91.)	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
	(2) 允许	110	自定义 TCP	目的: 3369/3389	源: 0.0.0.0/0	

- 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

* 资源模型:	请选择				^
	▲ ● 主机	>	SQL Server		O SQL Server2008及以上版
	O Web Server	>	🕞 GBase	>	
	O Application Server	>	🌖 达梦	>	
	○ 中间件	>	🍔 Redis	>	
	O 数据库		😑 Oracle	>	
			/ MariaDB	>	

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。

* 资源模型:	数据库 / SQL Server / SQL Server2008及	以上版本	∽ ?
O SqI Server连持	安信息		
* 数据库IP地址:	请输入IP地址	* 数据库端口:	1433
* 用户名:	请输入用户名	* 密码:	请输入密码
查询超时(秒):	15		
○ 主机连接信息			
* 主机模型:	Windows主机	* 监控协议:	SNMP v1/2 V
* IP地址:	请输入IP地址	* 端口:	161 A
* 只读共同体:	请输入只读共同体	* 读写共同体:	请输入读写共同体

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 数据车所在主机未被发现,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

₩ 南大通用 - GBase企业管理器	- 🗆 🛛
文件(F) 编辑(E) 视图(V) 工具(T) 窗口(W) 帮助(H)	
12.新建音响 🧉 🔄 🕼 🖉 🔖 🖈 🗈 🏦 🗶 🐕 🥵	
◎ 日注册的 □ 对象资源 □ □ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	ー ロ 隆樓 ※ S ー 日
CBase服务器 CBase服务器 CBase服务器 CBase 企业管理器简介	● GBase Server機能 ● GBase Server機能 ● Database ● Greigh Key ● Database ● Foreigh Key ● Database ● Foreigh Key ● Stored Procee ● Stored Procee ● Table ● User ● User ● View ● Sqlcii
密 妈(A): 服务器注册名称 服务器注册名称(N): 123.57.133.114 影试(E) 保存(V) 取消(C) 釋助(H) 7.10/1958(KH) OUL W中や115(35)ギャービジ達入)家。	
<) ()

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

Converight (2)	2004 2018	GRaca	A 11	righta	racartiad
	C)	2004-2010	UDase.	АП	memo	IESEIVEU.

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:\Use	rs\wang	qi>netsh fir	ewall show	portopenin	g
域 配計 端口	置文件的 协议	端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩	—————————————————————————————————————		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 酉 端口	记置文件 协议	的端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	一 肩肩肩肩肩肩肩肩肩 一 一 一 一 一 一 一 一 一 一 一 一 一 一	· 入入入入入入入入入入入入入		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)

Y	方向出	坊向				
Ŧ	动添加	快速添加全部编辑	Q、输入端口或者授权3	対象进行撞索		
	授权策略	优先级 〇	协议类型	講口范围 ①	授权对象①	
	⊘ 允许	8 1	自定义 TCP	目的: 80/80	源: 0.0.0.0/0	
	⊙ 允许	4	自定义 TCP	目的: 50000/51000	源: 0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	21	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
	(2) 允许	110	自定义 TCP	目的: 3389/3389	源: 0.0.0.0/0	

- 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

请选择	请选择				
<u> </u>					
O 主机		SQL Server		O GBase 8S v8.x及以上版本	
O Web Server	>	G GBase			
O Application Server		🥩 达梦			
○ 中间件		🥮 Redis			
○ 数据库		🗢 Oracle			
		🖌 MariaDB	>		

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。
* 资源模型:	数据库 / GBase / GBase 8S v8.x及以上版本		~ (?
Gbase连接信	息		
* IP地址:	请输入IP地址	* 端口:	3306
* 用户名:	请输入用户名	* 密码:	请输入密码
查询超时(秒):	15 ^		
主机连接信息			
* 主机模型:	Linux主机 ~	* 监控协议:	SSH协议 ~
* IP地址:	请输入IP地址	* 靖口:	22
* 用户名:	请输入用户名	* 密码:	请输入密码

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

🢡 🕞 GBase 8s 数据库 [5258] 数据库(2) ▼ 告警信息 (0)			℃ 15分钟▼ ⑧ ▼ ●
基本信息	1 <u>1</u> ⊮⊎	最近7天可用性		1
○ 名称: 123.57.133.114:5258	连续运行时间	10-21 10-22	10-23 10-24 1	0-25 10-26 10-27
○ 备注名: GBase 8s 数据库 [5258] 🗹				
O 版本: 8.3.81 ○ 字符集: utf8	6 ⁶⁰ 60 ⁶⁰ ⁶⁰	a * a	40 ⁵⁰ 60	总容量
O 安装目录: /opt/GBase8sMySql/Ser	20 20 10	- 2 ⁻ 2	20 80	59.25 06
O 数据目录: /opt/GBase8sMySql/Ser	- 6 80.4% 100 ¹⁰ 0% 100 ¹⁰	33.52% 10	0.9% 100	23.94 GB
O 日志目录: /opt/GBase8sMySql/Serv	系统CPU利用率 MySQL CPU利用	率 系统内存利用率	MySQL内存利用率	数据分区(61%)
6%/100/6/94	1-/-/-/-	32.0M/-/20	59/1/	13
连接使用率/最大连接数/已用连接数/剩余	未提交事务数量 / 当前死锁数 / 锁数量 / 锁等	查询缓存 / InnoDB缓存 / 线程缓存	字 打开文件数量,	/ 慢SQL数量 / 全表扫描数

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:\Use	rs∖wang	qi>netsh fir	ewall show porto	pening
域 配置 端口	置文件的 协议	端口配置: 流量方向	名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP TCP TCP TCP	 	入入入入入入入入入入入入	Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 曹 端口	記重文件 协议	的端口配置: 流量方向	名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩上的	入入	Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)

λ	方向出力	方向				
Ŧ	司添加	快速添加全部编辑	Q、输入端口或者授权;	的象进行搜索		
	授权策略	优先级 〇	协议类型	講口范围 ①	授权对象①	
	⊘ 允许	1	自定义 TCP	目的: 80/60	源: 0.0.0.0/0	
	② 允许	1	自定义 TCP	目的: 50000/51000	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	② 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
-	(2) 允许	110	自定义 TCP	目的: 3369/3389	源: 0.0.0.0/0	

- 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

* 资源模型:	请选择				
	 O 主机	>	SQL Server	>	O达梦 V7.x及以上版本
	O Web Server	>	🕞 GBase	>	
	O Application Server	>	🐠 达梦		
	○ 中间件	>	🍔 Redis	>	
	O 数据库		😑 Oracle	>	
			🖌 MariaDB	>	

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。

* 资源模型:	数据库 / 达梦 / 达梦 V7.x及以上版本		
)达梦连接信息			
* IP地址:	请输入IP地址	▲ 端口:	3306
* 用户名:	请输入用户名	* 麦码:	请输入密码
查询超时(秒):	15		
2 主机连接信息			
* 主机模型:	Linux主机 ~	* 监控协议:	SSH协议 ~
* IP地址:	请输入IP地址	* 靖口:	22 ^ ~
* 用户名:	请输入用户名	* 密码:	请输入密码

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

🌻 🋸 DAMENG 8 [5336] 表空间(1) 🔹 告罄			C 159# • @
▲本信息 ○ 名称: 123.57.133.114.5336 ○ 名称: 123.57.133.114.5336	5×3 /ver istellistretei	#267天可用性 10-28 10-29 10-30 10-31	11-01 11-02 11-03
 ○ Nt本: DM Database Server a64 V8 ○ 用告: - ○ 月時時: - ○ 月時時: 2020-10-29 10:41:56 	SigCrunne REEC Crunnes	5.23.14%	673/801 88469/8826669
5/5/2 表空间数量/数据文件数量/日志文件数量	.4м/541.97м/100м Log Buffer音量 / 内持始音量 / Buffer Cache音量	5/0/0 1/1 助政문/元幼政문/田寨助政문 - 田東助政会 - 田代政人法	Session政星
▮ 燈沖憩傘中率		1 內行使用趋势	
(%) 100 80 40 20		(M) 500 400 300 200 100	

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 数据车所在主机未被发现,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:\Use	ers\wan	gqi>netsh fi	rewall sho	ow portopenin	1
C:\Use	rs\wang	qi>netsh fir	ewall sho	w portopening	
域 配計 端口	置文件的 协议	端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩			Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 曹 端口	记置文件 协议	的端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩			Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_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)

λ	方向出	方向			
手动添加 快速添加 全部编辑			Q、输入端口或者授权对象进行搜索		
	授权策略	优先级 〇	协议类型	端口范围 ①	授权对象 ①
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0.0/0
	② 允许	-1	自定义 TCP	目的: 50000/51000	源; 0.0.0 .0/0
	⊘ 允许	1	自定义 TCP	目的: 21/21	源: 0.0.0.0/0
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	·源: 0.0.0.0/0
	② 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0/0
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0/0
	(2) 允许	110	自定义 TCP	目的: 3389/3389)便: 0.0.0.0/0

- 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

贝刷剂关生	请选择				
	O 主机	>	SQL Server	>	○ Redis v5.x及以上版本单机监控
	O Web Server		🕞 GBase		
	O Application Server		🝠 达梦		
	O 中间件		🥮 Redis		
	O 数据库		Oracle		
			🖌 MariaDB	>	

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。

○ Redis连接信息	1				
* IP地址:	请输入IP地址	* 靖口:			
* 密码:	请输入密码	查询超时(秒):	15		
○ 主机连接信息					
* 主机模型:	Linux主机	* 监控协议:	SSH协议 ~		
* IP地址:	请输入IP地址	* 端口:	22		
* 用户名:	请输入用户名	* 密码:	请输入密码		

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

1.5.5.1.22. 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:\Use	ers\wan	gqi>netsh fiı	ewall show	v portopen	nin
C:\Use	rs\wang	qi>netsh fir	ewall show	portopenin	ng
域 配置 端口	置文件的 协议	端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP	启启启启启启启启启启 用用用用用用用用用用用	入入入入入入入入入入入		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in
标准 曹 端口	记置文件 协议	的端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	。 居启启启启启启启启启 用用用用用用用用用用用	入入入入入入入入入入入入 入		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in

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)

Y	方向出江	方向				
Ŧ	动添加	快速添加全部编辑	9、输入端口或者授权3	國法正行搜索		
	授权策略	优先级 〇	协议类型	號口范围 ①	授权对象①	
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0.0/0	
	⊙ 允许	4	自定义 TCP	目的: 50000/51000	源: 0.0.0.0/D	
	⊘ 允许	4	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	21	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
-	(2) 允许	110	自定义 TCP	目的: 3389/3389	源: 0.0.0.0/0	

- 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

* 资源模型:	请选择				
	O 主机	>	쏅 SQL Server	>	○ PostgreSQL v11.x及以上版本
	• Web Server	>	GBase	>	
	 Application Server 	>	🌗 达梦	>	
	○ 中间件	>	쒤 Redis	>	
	○ 数据库		🕸 PostgreSQL		
			Oracle	>	

图 2-55 资源发现页面 87 / 127

● 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。

* 资源模型:	数据库 / PostgreSQL / Pos	stgreSQL v11.x	及以上版本	✓ ⑦ 发现前提	
PostgreSQL连	接信息				
* IP地址/域名:	请输入IP地址/域名		* 端口:	5432	
* 用户名:	请输入用户名		* 密码:	请输入密码	
查询超时(秒):	15				
 主机连接信息 					
* 主机模型:	Linux主机		* 监控协议:	SSH协议 ~	
* IP地址/域名:	请输入IP地址/域名		* 端口:	22 <u>^</u>	
* 用户名:	请输入用户名		* 密码:	请输入密码	
○ 维护信息					
责任人:	系统管理员				
供应商:	请选择		供应商负责人:	请选择 ~	

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:\Use	rs\wang	qi>netsh fir	ewall show	portopenin	g
域 配計 端口	置文件的 协议	端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩上	—————————————————————————————————————		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 酉 端口	记置文件 协议	的端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩上			Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)

Λ.	方向世	访问				
Ŧ	动添加	快速添加全部编辑	Q、 输入端口或者授权	対象进行搜索		
	授权策略	优先级 〇	协议类型	講□范围 ①	授权对象①	
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0.0/0	
	◎ 允许	-1_	自定义 TCP	目的: 50000/51000	源: 0.0.0/0	
	⊘ 允许	9 <u>1</u>	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
	(2) 允许	110	自定义 TCP	目的: 3369/3389	源: 0.0.0.0/0	

- 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

请选择			<u>^</u>
▲ O 主机	SQL Server	>	O Oracle v11.x及以上版本单机监控模
O Web Server	G GBase		
O Application Server	🥌 达梦		
O 中间件	🎯 Redis		
O 数据库	😄 Oracle	×	
	🖌 MariaDB	>	

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。

*资源模型:	数据库 / Oracle / Oracle v11.x及以上版	夜本单机监控模型	
Oracle连接信题	2		
* 数据库IP地址:	请输入IP地址	* 数据库端口:	1521
* SID:	请输入SID	* 用户名:	请输入用户名
* 密码:	请输入密码	查询超时(秒):	15
) 主机连接信息			
* 主机模型:	Linux主机 ~	* 监控协议:	SSH协议 ~
* IP地址:	请输入IP地址	* 端口:	22
* 用户名:	请输入用户名	* 密码:	请输入密码



 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。





● 点击资源后,进入资源概览页

修易维宝 首页 北约度用	(2011) 新始哲理 新始哲理 新始哲理 (2011) 新始哲理 (2011) 新始哲理 (2011) 新始哲理 (2011)
资 💡 📑 Oracle 11G [1521] 会话 表空间(3) → 告警信息 (1	◯ 159(♦▼) ◎ ▼ ◎ ▼
列 I 基本信息 Q 名称: 60.28.43 197:1521	■ 26 天 20 小时 建築論(7時間 10-21 10-22 10-23 10-24 10-25 10-26 10-27
 ○	
O 数据连编码: ZHS16GBK O 数据连角色: PRIMARY	*********************************
○ 活动会话数: 21 ○ 事务平均响应时间:	系统CPU转用率 数据在CPU利用率 然期时内存利用率 数据时内存利用率
I Oracle概范	C 0
服务器进程	
PGA ● ● ● ● ● ● ● ●	SGA 截氮库文件
专用 0.10桁脚	Buffer Cache 376632X8 Oblocks/P FR0:05 0K8 C115,2019 6011M8 Sci2884
21 — — — —	Buffer Cache 命中學 0.01blocks/修 1001blocks/修 0.01blocks/修
	99.86%。 当前 SGA 1032192K8 人间恢复 大小

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:\Use	ers\wan	gqi>netsh fi qi>netsh fir	rewall show por	ortopen	in ទ
域 配計 端口	置文件的 协议	端口配置: 流量方向	名	称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	启启启启启启启启启启	补站站站站站站站站站站站 站站		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 酉 端口	配置文件 协议	的端口配置: 流量方向	名	称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	一启启启启启启启启启启	入入入入入入入入入入入入入入		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in 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)

У	方向出方	向				
Ŧ	动添加	电速添加 全部编辑	Q、输入端口或者授权对象	教进行搜索		
	授权策略	优先级 〇	协议类型	端口范围 ①	授权对象①	
	⊘ 允许	8 1	自定义 TCP	目的: 80/80	源: 0.0.0/0	
	② 允许	1	自定义 TCP	目的: 50000/51000	源: 0.0.0.0/D	
	⊘ 允许	1	自定义 TCP	目的: 21/21	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 10200/10230	源: 0.0.0.0/0	
	② 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
	(2) 允许	110	自定义 TCP	目的: 3369/3369	源: 0.0.0.0/0	

- 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

以 发现					
*资源模型:	请选择				
	O 主机	2	SQL Server	~	O MariaDB v10.x及以上版本
	O Web Server	>	G GBase		
	O Application Server	>	🐠 达梦		
	O 中间件	>	🥮 Redis		
	O 数据库		Oracle	>	
			/ MariaDB		
					分明
					及现

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。

* 资源模型:	数据库 / MariaDB / Mar	iaDB v10.x及以上版	本	× ?
) MariaDB <u>连接</u>	信息			
* IP地址:	请输入IP地址		* 端口:	3306
* 用户名:	请输入用户名		* 密码:	请输入密码
查询超时(秒):	15			
) 主机连接信息				
* 主机模型:	Linux主机		* 监控协议:	SSH协议 ~
* IP地址:	请输入IP地址		* 端口:	22 ×
* 用户名:	请输入用户名		* 密码:	请输入密码

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。





• 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

域 配置 端口	置文件的 协议	端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	肩肩肩肩肩肩肩肩上			Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_31637_in
标准 酉 端口	记置文件 协议	的端口配置: 流量方向		名称	
33060 3306 8879 8878 21346 68 67 21735 9876 31637	TCP TCP UDP UDP UDP UDP UDP TCP TCP TCP	启启启启启启启启启用用用用用用用用用用用用用用用用用用用用用用用用用用用用用用	动站站站站站站站站 站站站		Port 33060 Port 3306 zapya_NET_FW_IP_PROTOCOL_UDP_8879_in zapya_NET_FW_IP_PROTOCOL_UDP_8878_in zapya_NET_FW_IP_PROTOCOL_UDP_21346_in zapya_NET_FW_IP_PROTOCOL_UDP_68_in zapya_NET_FW_IP_PROTOCOL_UDP_67_in zapya_NET_FW_IP_PROTOCOL_TCP_21735_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_9876_in zapya_NET_FW_IP_PROTOCOL_TCP_9361_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)

Λ.	万向出	方向				
Ŧ	动添加	快速添加全部编辑	Q 输入端口或者授权对	象进行搜索		
	授权策略	优先级 〇	协议类型	端口范围 ①	授权对象①	
	⊘ 允许	81	自定义 TCP	目的: 80/80	源: 0.0.0/0	
	② 允许	4	自定义 TCP	目的: 50000/51000	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 21/21	源; 0.0.0.0/0	
	⊘ 允许	<u>.</u>	自定义 TCP	目的: 10200/10230	源; 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 20092/20092	源: 0.0.0.0/0	
	⊘ 允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
	(2) 允许	110	自定义 TCP	目的: 3389/3389	源: 0.0.0.0/0	

- 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。

* 资源模型:	请选择				
	▲ O 主机	>	GBase	>	O MySQL v5.x及以上版本
	O Web ServerO Application Server	> >	e Redis	>	
	○ 中间件 ○ 数据库	>	😑 Oracle <i> M</i> ariaDB	> >	
			🕵 MySQL		

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

					G 15919 - @ + @
#+@#		() RE7天可用性		فكره والمتحدين	
) 名称: 121.36.175.212) 兼注名: 121.36.175.212 [半方云服务務] 📝		09-19			
) 昭作系統後行版法: centos_7.6.1810) 昭作系統紀末: Linux 3.10.0-1062.1.1.el7.a86_64	5.64%	. 50.63%	0.01 / 0.08 CPU58E1999/5999	87年度 57445 GB 日初 7.58 GB	参容量 0.0 KB 日用 0.00 KB
	CTUNER	P3存利用書 Swap Usage		918 (1.32%)	Swap Space (0%)
EXCOUNTEER		41- C @ 1 ERATE	198		
80 60		3			
20 21:10 21:25 21:40 21:55 22:10 22:25 2	240 2255 23:10 23:25 23:40 23:55 00:10	0025 0040 00.55 00:	0 00:15 00:20 00:25 00:30 00:	IS 0040 0045 00.50 C	0.55 01:00 01:0
20 0 21:10 21:25 21:40 21:55 22:10 22:25 2 21:50 21:25	2440 2255 23.10 23.25 23.40 23.55 00:10	0025 0040 0055 000	0 00:15 00:20 00:25 00:30 00:	IS 0040 0045 0050 0	0.55 01:00 01:0
70 2110 2125 2140 2155 2210 2225 2 REGACHU TOPS IPA 1110 REGion BES/Miniford York	2-40 2255 23:10 23:25 23:40 23:25 00:10	0025 0040 0055 00 0 0055 0055	0 00:15 00:20 00:25 00:30 00: 1095	15 00.40 00.45 00.50 0 56m -00 + UseConcMarkSweepGC -XXCANSMI	055 01:00 01:0 C B44.63M tingDccapancyFraction175 - D4M
20 21/0 21/0 22/0 2	244 2255 2246 2255 2240 2255 0010 2566 8062566 021144ContMakSongSC 00CMI00 0566 8062566 021144ContMakSongSC 00CMI000	0025 0040 0055 00 10205 0040 0055 00 10205 0040 0055 jan 10205 jan 10205 jan jan	9 00:5 0020 0025 0030 00 0093	is 00.40 0045 00.50 c 35m XX + UuccuncharbineeppC XXXXXIII/4500 4/processed - Doos sour paragrammet/janceme 517.455M	ess 01:00 01:0 C BLACSM thigOccupancyFraction:75 DLM gott=2163 - Dromsauroma

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

	Advect Application Application <t< th=""><th></th><th></th></t<>		
网路接口接收包裁趋势	网路接口接收速率趋势	网路接口发送包数趋势	网路接口发送速率趋势
◆ 新建规图			

图 2-69 选择视图

1.6.2 自定义视图

● 点击新建视图按钮

	Pro- Instituti Dipo Mylocys Indian andre Attinisticandologi California. Bélandi H, Belanian M, Belanian J, Belanian M, Belanian J, Belanian M, Belanian J, Belanian M, Belanian		Robert Big State B
系统CPU利用率趋势	进程占CPU TOP5	系统内存使用趋势	进程占内存 TOP5
Non- Non- <th< td=""><td>All some take same same state same</td><td>The second secon</td><td></td></th<>	All some take same same state same	The second secon	
网路接口接收包数趋势	网路接口接收速率趋势	网路接口发送包数趋势	网路接口发送速率趋势
新建视图			
新建規图			

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。

* 应田夕段•	完全管理系统		
121011199-	相音自建制机		+
* 负责人:	高明 >	排序号: 1 <u>∧</u>	图标上传
URL:	POST V HTTP V	192.168.0.10/login.do	
标准响应时间:	3000 (這秒)		
请求头部:	参数名	参数值	操作
	Content-Type	application/json	+ 🗉
	请输入	请输入	+ =
请求参数:	💿 Form Data 🏾 🔵 JSON		
	参数名	参数值	操作
	userName	admin	+ 🕯
	password	1qa2ws3ed	+ 🗉
成功返回关键词:	登陆成功		(
备注:	请输入备注信息		

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

	ere leter skrat		
新福田	🔗 会议运营管理系统 🔋		
	47105155145(小沙平廊站建 唐泉)	47 105 184 210 1 かいデビスがあ、市区 1	
	20174 S 0% S 17.30%	705.94K8ps 0 0% 00 13.10%	
47.105.155.145 (会议元服装器-商品) 🕴 🚺 👔 👔 👔 👔	108) 💡 65.99K8ps		
	er (50400)		
	75.3958 65.39588ps		
	@QUESHIPT [10000]		
	Constant and a second s		
	node2		
	State and a set of the		
	8口管理系统 🔤 综合化维管理系统 💭 监控系统工具集 🔛 製能	全委应用运用管理平台 😂 宿舍管理系统	

图 3-3 编辑业务应用

● 点击模块信息

┃ 编辑业务应用 - 会议运营管理系统		×
基本信息 模块信息		+ 新建
名称 🖨	备注	操作
		4

图 3-4 模块信息页面

● 点击新建按钮填写模块名称
┃ 编辑业务应用 - 会议运营管理系统		×
基本信息 模块信息		+ 新建
名称 🗢	备注	操作
	暂无数据,点击新建	

┃ 新建 - 模块		×
* 模块名称:	请输入名称	
排序号:		
备注:	请输入备注信息	
	连接测试 · · · · · · · · · · · · · · · · · · ·	2

图 3-5 新建模块信息

● 确定保存后点击名称编辑模块内容

┃ 编辑业务应用 - 宿舍管理系统	×	
基本信息 模块信息		十新建
名称 ◆	备注	操作
宿舍分配规划	宿舍分配规划	ŵ

* 模块名称:	宿舍分配规划		
排序号:			
* URL:	POST V HTTP V	192.168.0.10/sg-admin-app/schemaMain/getList.do	
标准响应时间:	3000 <u>^</u> (毫秒)		
请求头部:	参数名	参数值	操作
	Content-Type	application/json	+ 🛍
请求参数:	💿 Form Data 🏾 🔵 JSON		
	参数名	参数值	操作
	year	2020	+ 🛍
	stuType	edu-level-001	+ 🛍
* 成功返回关键词:	查询规划信息成功		
备注:	请输入备注信息		

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。

		and the second se					
梁和图· © 可用度 97.73% (目中体系	組数 99 分		议运宫官埋杀犹 1				
			47.105.155.145 (会议元服务器-青岛] 💦 💡	47.105.184.21	0 [会议元服务器·青岛] 💡	
				-4000	> 👩 sumo	RR91: [4000]	
			20150年 2015年	76.97%		. 🔮 77.24%	
17.105.155.145 [会议云服务器·青岛] 👘 💡	123.56.94.138	NNM 云服务器-北京)	521K8ps				
会议主Web Server [443]	2013時期 16.46KBps 16.46KBps	RESURAPP Server [10410]					
	C I I MA	0 71605	お試修業 5.21KBps 会议ES生計[100	会议云服务器-青岛] ? 00]			
			node1				
				98%			
			node2	-			
				20.8			
			Concel	97%			
				·			

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。

资源	输入关键字进行过滤	指标	输入关键字进行过滤	
÷ 🙏	121.36.175.212 [华为云服务器]	▼ 性	能指标组	
	分区 (3)		CPU利用率 [%]	
• 1	CPU (4)			
	cpu0			
	cpu1			
	cpu2			
	сриЗ			
▶	网卡 (1)			
► F	硬盘 (2)			
- E 🙏	47.105.184.210 [会议云服务器-青岛]			
	华为云App Server [8162]			
🕞 🕨 😽	华为云ES集群 [10000]			

a			 121.36.175.212 [华	为云服务器]	
↓ 47.105.184.210 [会议 华为云ES集群 [10000	云服务器-育岛]]		华为云App Sei	rver [8162] 👜 -	
node1	8 -	发送速率 23.97KBps			
node2	0 -				
node3	0 -				



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

Ⅰ 选择业	/务应用				×
	🛱 HR会议管理系统	🛱 NNM会议管理系统	🛱 会议接口管理系统	🛱 会议运营管理系统	
;	📮 宿舍管理系统	智能业务应用运维管理 平台	😝 监控系统工具集	🙀 综合代维管理系统	
					ſ
ţ					
				确定	2

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



资源视图 首页自定义视图				
▼ 👃 Linux主机		14 N271 Blas Miljon indie inder biskontekant Babia. Behlit 15		aa Robii Ubja Milya kulla kulla kulla kulla kulla kulla kulla kulla
121.36.175.212 [华力云服务器]				
122.112.210.224 [平乃云版另番] 123.56.94.138 [NNM元昭各罢-北京]	THE TAX OF THE THE THE THE THE THE THE THE THE	yean N N: Disperd MysRipherbered subdets upon Andre 2	CH 101 100 100 100 101 104 104 105 10 106 100 100	
123.57.229.89 [华为云服务器]	系统CPU利用率趋势	进程占CPU TOP5	系统内存使用趋势	进程占内存 TOP5
47.104.106.164 [会议云服务器-青岛]	a Financia da Antony ella		a Annually a Number	
47.105.155.145 [会议云服务器-青岛]			200 200 201 201 201 201 201 201 201 201	2001 2007 2007 2007 200 200 200 200 200 200 200 200 200
47.105.184.210 [会议云服务器-青岛]	NB0 23 6.6 MB 6.3 Edulus 22.6 3 3 3 Plana 023 401 40.6 6.61		MARA 20 514 Fill 518 R.Mulliong 22.04 3 3 3 R.Samp 20.05 40.09 40.01 40.01	3830 300 646 414 6.14 Abbitmay 0278 3 3 5 Planear 0278 4.37 4.53AC 4251
60.28.43.197 [IDC服务器]	网路接口接收包数趋势	网路接口接收速率趋势	网路接口发送包数趋势	网路接口发送速率趋势
▶ 📒 Windows主机				
▶ 🔊 Nginx				
► 💐 Tomcat				
▶ [Ħ// Jetty				
ElasticSearch				

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



4.1 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

修易维宝 前 · · · · ·	业务应用 资源管理 告解管理 維給管理	系统管理
 · (10.1200.162.134 [阿里云服务器] · (阿里云服务器) · (阿里云般器库 [4000] · (120.132.61.202 [易后台服务器] · (121.36.175.212 [华为云服务器] · (121.36.175.212 [华为云服务器] · (121.122.10224 [华为云服务器) · (121.122.10224 [华为云服务器] · (121.122.10224 [华为云服务器) · (121.122.10224 [华)) · (121.122.10224 [Ф)) · (121.122.10224 [Ф)) · (121.122.10224	■ 2 現後300 2 月 2 月 3 月 3 月 3 月 3 月 3 月 3 月 3 月 3	○ 15分钟 ③ ● ● 2 10-23 10-24 10-25 10-26 約名量 11.59 GB ○ ○ ○ 141.59 GB ○ ○ ○ ○ ●
 ▲ 47.105.184.210 [会议无能务器:青岛] [●] ▲ 60.28.43.197 [DC服务器: \ ● ● 60.28.43.210 [IDC服务器: Win2018] [●] ● 60.28.43.210 [IDC服务器: Win2012] [●] 	4H+ C ◎ (6) 3 2 1	1H • C © • \$480.00 • \$400.000

图 5-1 资源管理页面

● 进入告警设置菜单

Ŵ		· 业务应用 一 资源管理	合整管理 運給管理 养	統管理 您好!系统管	■□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
资源	📍 🗼 101.200.162.134 [阿里云服务器] 告警信	S (0)		011	559# 🗝 🎯 🔹 🕺
列表	 Ⅰ 基本信息 ○ 谷称: 101200.162.134 ○ 省注名: 101200.162.134 [阿里 	123天22小时 连续运行时间	₩近7天可用性	10-23 10-24	监控配置 告警配置 视图配置
	 一提作系统发行版本: centos_8.1.19)提作系统版本: Linux 4.18.0-147 	8.04% w	олоб / 0.15 общат сридатание / 534	総容量 141.59 GB 40.99 GB	总容量 0.0 KB 已用 0.00 KB
		PU利用率内存利用率	Swap Usage	分区(28.95%)	Swap Space (0%)
	Ⅰ 系统CPU利用率趋势	4H + Q	◎ 系统内存使用趋势		1H+ Q @
	(%) 100 80 60 40 20		(G) 3 2 1	- 5 88	Aluter - Sanc Hunter

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。

主资源	4 严重告警			
,分区	告警标题	告警类型	告警条件	操作
• 网卡	Linux主机-SSH远程登录失败	可用性	主机可用性 = -1 并且 持续时间>5分钟	Ø 🕯
▶ CPU ▶ 硬盘	Linux主机-系统负载过高,有可能导致系统响应变慢卡顿	性能	CPU平均负载(1分钟) > 4 && CPU平均负载 (5分钟) > 4 并且 持续时间>10分钟	
	道 整示告警			
	告警标题	告警类型	告警条件	操作
		· · · · · · · · · · · · · · · · · · ·		

图 5-3 告警配置页面

▋新建	- 告警配置		×
	* 告警类型:	可用性 性能 配置	
	* 告警标题:	测试性能告警	
	告警条件:	请选择 ∨ 请选择 ∨ 请选择 ∨ 请输入 + □	
	持续时间:		
	关联视图:	+添加视图	
	告警帮助:	请输入帮助内容	
		· · · · · · · · · · · · · · · · · · ·	1

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。

1户管理	系统管理 > 消息通知配置			
又嚴管理				
#思通知配置	自用消息通知	配置后,当出现告警或者巡检任务执行完毕的时候将通过配置的方式发送消	總提解.	
	* 启用告誓通知:	可用性告警 性能严重告警 全部告警信息		
	* 启用巡检结果通知:			
	* 通知方式:	企业操信应用满思 企业微信群机器人 钉钉群通知机器人	钉钉工作消息通知 SMTP邮件 第三方接口	
	A 7500 L 10 57-	TEQT	* 75/01 J #070s Loc1/01/63 com	
	ⅈ Aita		OCTTAMPEL ISSUE 103.COM	
	* SMTP服务地址:	smtp.163.com	* SMTP服务端口: 25	
	• SMTP张号:	test	* SMTPRE	
	* 是否需要加密: (* 邮件编码格式: 💿 UTF-8 🌑 GBK 💿 GB2312	
	* 邮件标题:	请输入邮件标题		

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/zx1782340680/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

① 07月2日日 角色列表 ● 基本信息 列用信息 26 伊班希哲理 近め田田の からたがい 近め田田の からたがい 近め田田の からたがい 近め田田の からたがい がら田田の からたがい がら田田の からしい からしい がらし、 が がらし、 が がらし、 が がらし、 が がらし、 が がらし、 が が	
3 供菜商管理 2 浜鉄管理页 2 浜鉄管理页 2 浜鉄管理页 3 浜鉄管理页 3 浜鉄管理页 3 浜鉄管理页 1 1 3 浜谷電辺 4	
消除意識UNU語 加速になる 加速になる 加速になる 約, DCS信息 損除号: 1 1 角色編述: 系統管理员	
Ap. DCS信息 第6号: 1 第6号: 第6号: 第6号: 第6号: 第6号: 第6号: 第6号: 第6号:	
角色描述: 系统管理员	
	应用

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

偷易维宝 🦯	前気 12名应用 刻遊告理 品名告理 近始告望 回来主张 系统告理 55551 mlp.demo ☆ ③ ① 〓 〇
久 用户管理	■ 系統管理 > 化限管理
③ 权限管理	角色列表 (7) 基本信息 (7) 供信息
848 供应商管理	系统管理员 金融合合合 系统管理员
□ 消息通知配置 品 DCS信息	
	角色/翻译 : 系统管理员
	ITAL

图 7-2 权限管理页面

● 输入基本信息后, 点击应用

< 用户管理	系統管理 > 权限管理	
② 权限管理	角色列表(基本信息 权限信息
å 供应商管理	系統管理员	2 <u>8 6 2 時</u> 彩坊管理日
90 POUR		角色描述: 系统管理员
		RA .

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

偷 易维宝	首页业务应用资源管理	音音管理 通知管理 医维利波 系統管理 初日 100 (⑦) 20 (⑦) 20 (⑦) 20 (⑦) 20 (⑦) 20 (⑦) 20 (⑦) 20 (⑦) 20 (⑦) 20 (⑦) 20 (⑦) 20 (◎) 20 (
久 用户管理	系统管理 > 权限管理	
⑧ 权限管理	角色列表 🕣	基本信息 权限信息
。 《 供应商管理	系统管理员	
💬 消息通知配置		▼ 业务应用 ▼ 新建业务应用
。 DCS信息		♥ 資源管理
		· 告罄告理 · · · · · · · · · · · · · · · · · · ·
		● 120月1日第 ● 第1法 ● 1113年 ● 1137年 ● 11374
		☑ 权限告理
		☑ 供应商管理 ☑ 新建 ☑ 圖停用 ☑ 新建维护人员
		Ra Ra

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

0 田山祭理	- 系統管理 > 用户管理						
		たな(手作用)サイ)神経(0 40-25				1 22
 权限管理 	±nµX32 ∨ IIJ#II/3	主有/于小亏近门保闲级					T an
治 供应商管理	姓名◆	性别 ◆	手机号 🗢	● 御道 ◆	用户名 ◆	角色 🗢	操作
河 消息通知配置							启用
⊗ DCS信息							

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

▮新建-用户信息				×
* 姓名:	张三	* 手机号:	1300000000	-
*密码:		1133:		
		企业发信号:	清榆入企业微信号	
钉钉账号:	请输入钉钉账号			
* 角色:				

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。

						东建记维州安	
						新建运维档条	
						[##] 1) bosines#P#: ###W. #B#W.	2
	1 988 - 1501P12				×		
	* Extense: © 200	1-09-10 18:40 포 G	2021-09-10 18:45	天型: 交易部			
	* 医糖人袋: DEMO	0 🕑 1631		DR 3	and the second sec		
	-			安 期	\$5		
	JIRKAS HEL	JT 20.001 9 1 2000 . JIM		HE RE			
	X取业务应用: MTP-2	音管理系统 💿 🛛 MTP-BUSI	NESS有户编目理系统《 图 活版				
	关联基础资源: MTP 测	第世理系统 [50400] ◎ ▶	ATP 812有小编管理系统 [50408] ③ [14	A 10			
	* 尚華: [第次 1) bu 分類 2) od 等天 考測 見 記 規 元 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	23 innex著件篇: 主義、 去律道王中心, 政方式 in加強領: 増理均夫世示領責行主、並示 確定,年1, 増加約責行主、並示 i示 3 () 23 stymeeting=bit=0.1.0=5005	№孝戸 料面が決別済戸 丹直後回方転 107: jar				
					82		

图 8-1 运维档案