APEX IT 综合管理系统 v5.6.7.x 配置手册

本手册指导如何对 IT 环境中各种需要被监控的目标资源进行正确的配置，以达到可被 APEX IT 综合管理系统监控的目标。

研发中心 - 文档开发组 2014 年 1 月 14 日更新

1. 目录

2. 说明

本文档按照 IT 资源的类型，分门别类列出监控的前置条件及配置步骤，未配置或配置错误可能导致无法监控或不能获取特定的监控指标。

3. 修订记录

修改内容	修订人	说明
起草	崔文俊	
增加网络设备的监控说明，第 4 到 16 章节； 增加第 42 章，可监控 EMC VNX/Symmtrix 系列磁盘阵列	崔文俊	2013 年 11 月 28 日更新
增加第 50 章节，描述如何对 HP EVA4400/6400 磁盘阵列进行监控	王颂	2013 年 12 月 3 日更新
第 17 章节，Linux 环境下修改 tomcat 启动脚本文件 catalina.sh，去掉了添加参数中多余的空格	王锋	2013 年 12 月 18 日更新
新增第 51 章节，设备间链路发现对设备本身的要求	崔文俊	2013 年 12 月 25 日更新
新增第 52 章节，接收第三方系统发送的告警； 新增第 53 章节，将告警通过 snmp trap 的方式转发给第三方系统	崔文俊	2014 年 1 月 14 日更新

4. 通用 SNMP 网络设备

如果设备支持 SNMP 且兼容 RFC1213，均可以通过 SNMP 协议对其进行监控，但只能监控一些常规参数：

1. Ping 判断设备是否在线
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量
4. Ping 判断设备的 ICMP 响应延时和丢包率

5. Cisco 设备

可通过 SNMP 协议监控 Cisco 交换机、路由器、防火墙等网络设备的运行状态和链路流量，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量
4. 监测设备的 CPU 使用率，内存使用率

6. 华为设备

可通过 SNMP 协议监控华为交换机、路由器设备的运行状态和链路流量，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量
4. 监测设备的 CPU 使用率，内存使用率

7. 中兴设备

可通过 SNMP 协议监控中兴交换机、路由器设备的运行状态和链路流量，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量
4. 监测设备的 CPU 使用率，内存使用率

8. H3C 设备

可通过 SNMP 协议监控 H3C 交换机、路由器设备的运行状态和链路流量，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量
4. 监测设备的 CPU 使用率，内存使用率

9. NetScreen 防火墙

可通过 SNMP 协议监控 NetScreen 防火墙设备的运行状态和链路流量，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量

4. 监测设备的 CPU 使用率，内存使用率

10. Juniper 设备

可通过 SNMP 协议监控 Juniper 交换机、路由器设备的运行状态和链路流量，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量
4. 监测设备的 CPU 使用率，内存使用率

11. 博达设备

可通过 SNMP 协议监控博达交换机设备的运行状态和链路流量，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量
4. 监测设备的 CPU 使用率，内存使用率

12. 神州数码设备

可通过 SNMP 协议监控神州数码交换机设备的运行状态和链路流量，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量
4. 监测设备的 CPU 使用率，内存使用率

13. 天融信防火墙

可通过 SNMP 协议监控华为交换机、路由器设备的运行状态和链路流量，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量

4. 监测设备的 CPU 使用率，内存使用率

14. 锐捷网络设备

可通过 SNMP 协议监控锐捷交换机、路由器设备的运行状态和链路流量，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可，包括：

1. Ping 判断设备是否在线，ICMP 响应延时和丢包率
2. snmp get 判断设备是否在线
3. 监测设备接口流量、丢包、错包、组播、单播、广播流量
4. 监测设备的 CPU 使用率，内存使用率

15. F5 Big-IP 负载均衡设备

可通过 SNMP 协议监控 F5 Big-IP LTM 8900 应用交付控制硬件平台，在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可。

16. Radware 负载均衡

可通过 SNMP 协议监控 Radware AppDirector 应用加速设备，该设备可为基于 Web 和 SSL 的应用提供端到端性能加速。

AppDirector 的加速技术包括 SSL 卸载、Web 压缩、静态和动态内容缓存、TCP 优化与带宽使用量控制技术，以提供快速的应用和事务响应时间，以及跨越各类介质（如蜂窝连接、无线网络和宽带连接）提供最佳的体验质量(QoE)等。

在设备上使能 SNMP Agent 并配置好 SNMP 读共同体即可。

17. Tomcat

支持通过 JMX 管理协议监控 Tomcat5.0.x、5.5.x 和 6.x 版本的应用服务器。

1. Linux 环境：

修改启动脚本文件，$TOMCAT_HOME\bin\catalina.sh，添加下列参数：

JAVA_OPTS=“$JAVA_OPTS –Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=12345
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false

-Djava.rmi.server.hostname=服务器的 IP 地址

参数加入位置，如下图：

a). Tomcat5.5

b). Tomcat6.0

2. Windows 环境：

打开%TOMCAT_HOME%\bin\catalina.bat 文件，加下列参数：
set JAVA_OPTS=%JAVA_OPTS%
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=12345
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=服务器 IP 地址

参数说明

- 端口‘12345’可根据需要进行修改，且该 port 就是在添加 TOMCAT 资源页面中需要的 JMX 监听端口，其它参数值请不要修改。

- 参数 hostIP 即为 Tomcat 所在主机的 IP，如果不配置这个参数，则有可能在添加被监控的资源是报 java.rmi.ConnectException: Connection refused to host: 错误。

Tomcat 做成 windows 服务之后使用 JMX 监控的配置

在[HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\ITSM\Parameters\Java]下修改 Options 参数，添加如下内容（图 2）：

-Dcom.sun.management.jmxremote

-Dcom.sun.management.jmxremote.port=1090

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

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

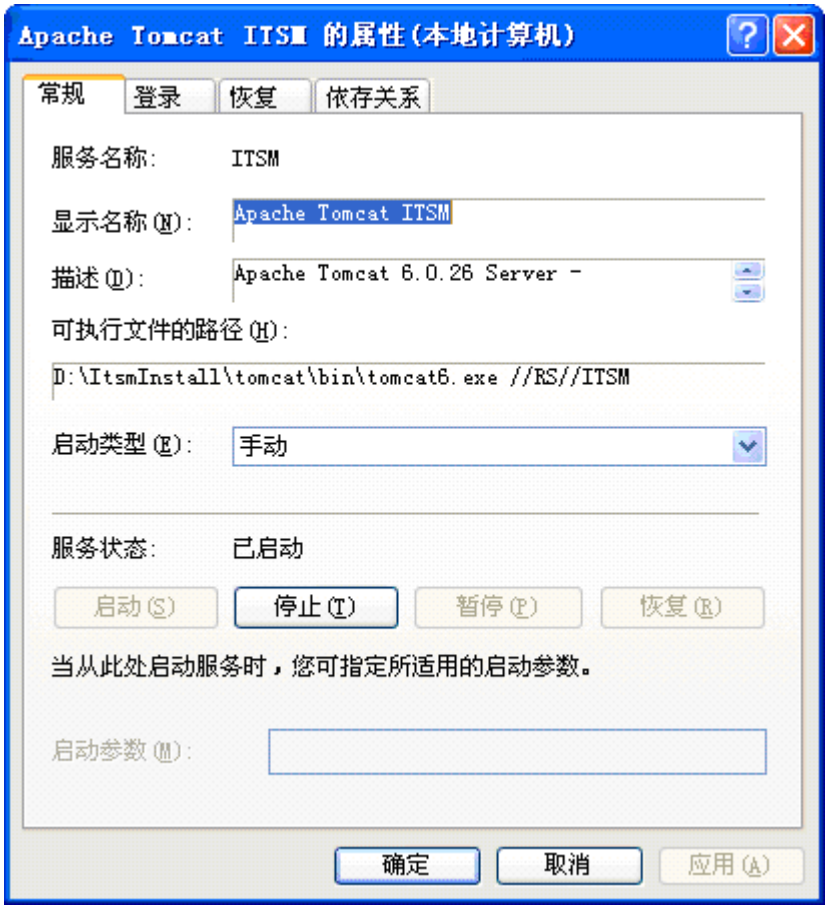
修改后测试发现可以连接，但是修改注册表毕竟不方便（当然可以写成.reg 文件直接让工程师去执行）。再查一下修改 tomcat 参数的文章，说到可以利用 tomcat6w.exe 来修改参数。

在 tomcat/bin 下面有 tomcat6.exe 和 tomcat6w.exe，其中 tomcat6.exe 自然是服务运行时必须的文件。曾经用过 jbuilder 且使用 jbuilder 的原理来把 jar 包生成 exe，所以对这个带 w 的 exe，第一印象就是对应的窗口化的程序。双击 tomcat6w.exe 执行，提示找不到服务 tomcat6。

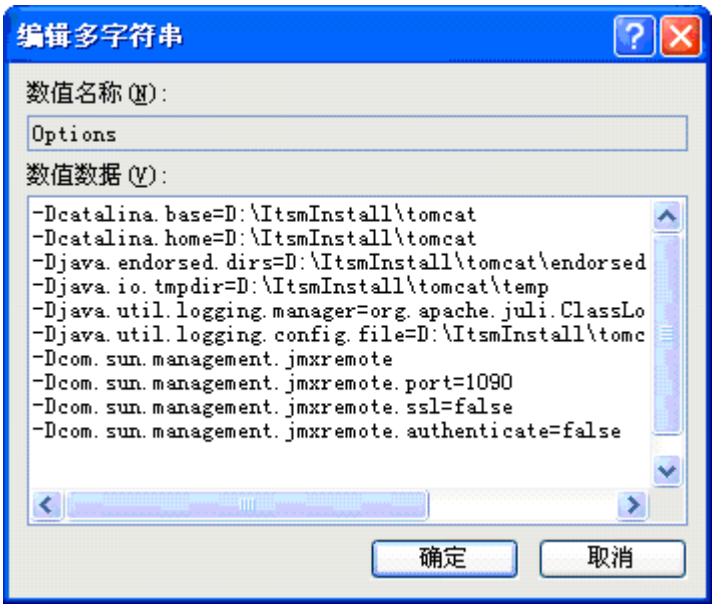
我理解 tomcat 默认会把服务注册为 tomcat6，而我们使用了 service install ITSM，注册后的服务是 ITSM，于是鬼使神差的就把 tomcat6w.exe 复制了一份改名为 ITSM，双击执行，打开了 ITSM 服务的配置界面（图 3）。界面里的 Java 选项卡中发现 java options 中已经有了 JMX 相关的参数。此时才意识到原来这里的设置就是对应的注册表中设置的那些参数。

至此，对于 tomcat 的参数设置终于明了，也意识到在 catalina 里面配置的增大 jvm 内存的参数，在注册为服务后，其实也没起作用。

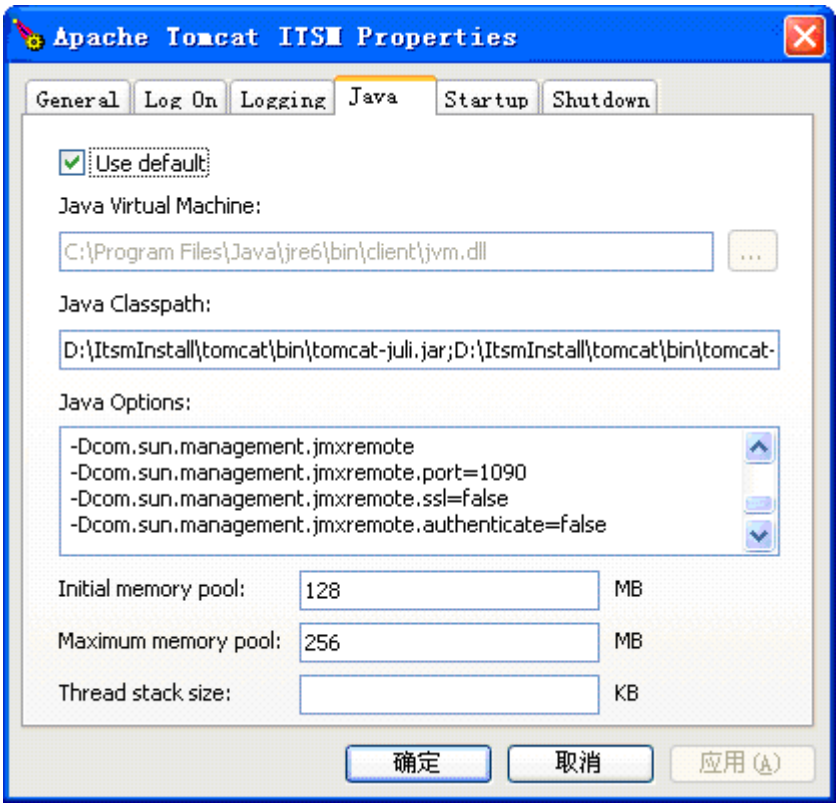
后来又测试了一下，删除 tomcat6w.exe 对服务并没有影响，它只是个纯粹的图形化的配置界面。当然 tomcat6.exe 是不能删的，删了服务肯定就无法启动了。


Apache Tomcat ITSM 的属性(本地计算机)
常规
登录
恢复
依存关系
服务名称:
ITSM
显示名称(N):
Apache Tomcat ITSM
描述(D):
Apache Tomcat 6.0.26 Server -
可执行文件的路径(H):
D:\ItsmInstall\tomcat\bin\tomcat6.exe //RS//ITSM
启动类型(E):
手动
服务状态:
已启动
启动(S)
停止(T)
暂停(P)
恢复(R)
当从此处启动服务时，您可指定所适用的启动参数。
启动参数(M):
确定
取消
应用(A)

（图 1）


编辑多字符串
数值名称(N):
Options
数值数据(V):
-Dcatalina.base=D:\ItsmInstall\tomcat
-Dcatalina.home=D:\ItsmInstall\tomcat
-Djava.endorsed.dirs=D:\ItsmInstall\tomcat\endorsed
-Djava.io.tmpdir=D:\ItsmInstall\tomcat\temp
-Djava.util.logging.manager=org.apache.juli.ClassLo
-Djava.util.logging.config.file=D:\ItsmInstall\tomc
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=1090
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
确定
取消

（图 2）



（图 3）

3. 配置完后需要重启 TOMCAT 服务才能生效

4. 防火墙配置

如服务器防火墙已关闭，则无需配置下面内容，

vi /etc/sysconfig/iptables

编辑 iptables,加入新一行内容：-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 12345 -j ACCEPT

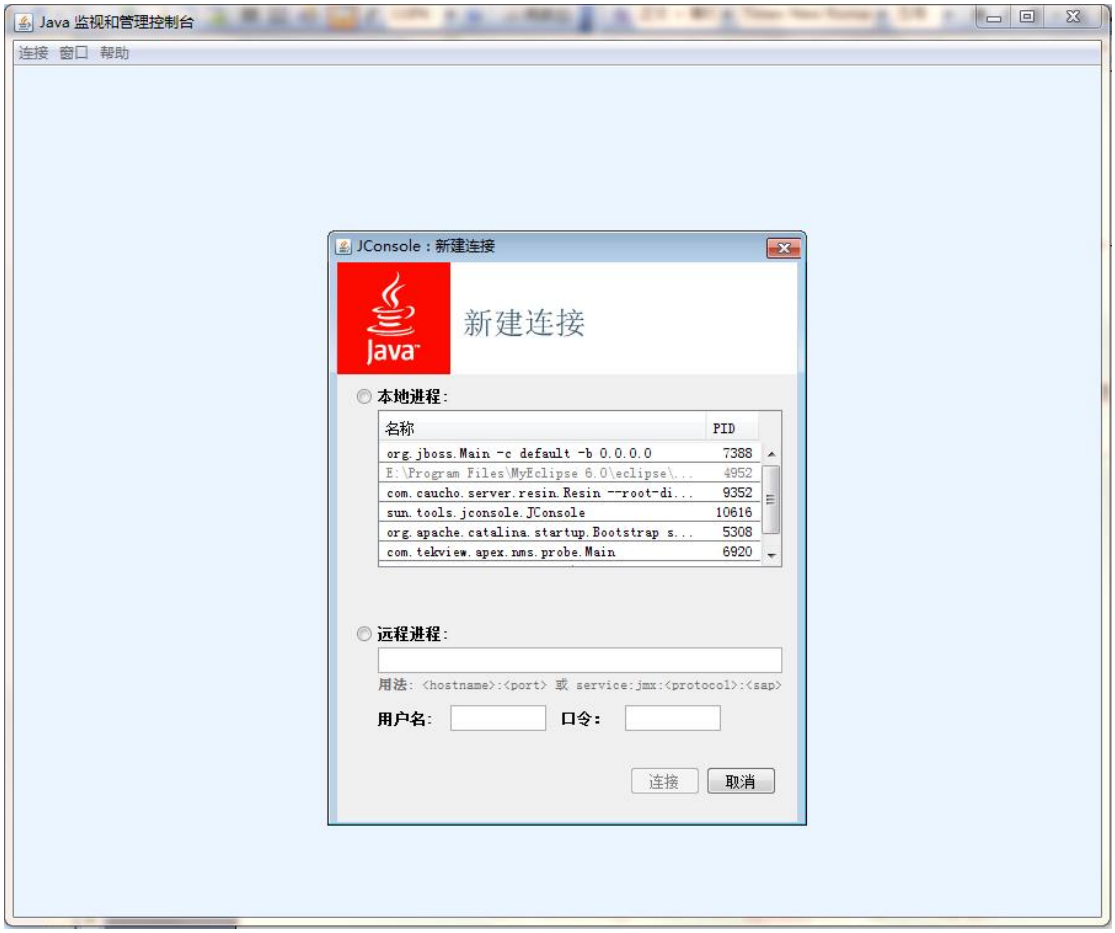
5. 验证配置及 TOMCAT 启动是否成功

1）用命令查看一下配置的端口和服务是否连通：

Netstat –an | grep 12345

2）如 TOMCAT 成功启动后，可通过 JCONSLE 来查看刚才配置的参数是否成功，操作步骤如下：

a). 直接在命令行中键入 JCONSOLE 命令，会弹出下窗口界面：



b). 选择远程进程，输入 Tomcat 服务器所在 IP 及在上面参数配置的端口号，用户名和密码不用填。格式如下：

192.168.0.21:12345

c). 点击连接，如果连接成功，说明配置正确。如不成功，则会返回连接超时提示。

6. 注意事项

1） 所有参数需放在同一行，每一参数之间用空格隔开。

2） 配置的端口不能已被占用。

18. JBoss

目前且支持 JBoss4.2.X、5.0.X、 5.1.X、6.0.X、6.1.X

18.1. JBoss 4.2.X

Linux 环境

打开%JBOSS_HOME%\bin\run.sh 文件，加入下列参数。

JAVA_OPTS =” $JAVA_OPTS -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=12345
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=IP”

参数位置，可放在 JAVA_OPTS="-Dprogram.name=$PROGNAME $JAVA_OPTS"这一行的下面

Windows 环境

参数：

set JAVA_OPTS=%JAVA_OPTS%
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=12345
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname= IP

参数位置

可放在 set JAVA_OPTS=%JAVA_OPTS% -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 这一行下面。

参数说明

端口‘12345’可根据需要进行修改，且该端口就是在添加 JBOSS 资源页面需要的 JMX 监听端口， 其它参数值请不要修改。

参数 hostIP 即为 JBOSS 所在主机的 IP, 如果不配置这个参数，则有可能在添加被监控的资源是报 java.rmi.ConnectException: Connection refused to host: 错误。

修改 HTTP invoker service 服务端口

打开%JBOSS_HOME%\server\default\deploy\http-invoker.sar\META-INF\jboss-service.xml 文件

1) 保证该配置文件中的 HTTP 访问端口与 HTTP 应用服务端口一致，例如 NM Server 应用的访问端口是 82，那么 jboss-service.xml 文件的 HTTP 访问端口也应为 82。修改如下图。

2) UseHostName 属性值改为 false, 如下图：

```
<!-- Expose the Naming service interface via HTTP -->
<mbean code="org.jboss.invocation.http.server.HttpProxyFactory"
   name="jboss:service=invoker,type=http,target=Naming">
   <!-- The Naming service we are proxying -->
   <attribute name="InvokerName">jboss:service=Naming</attribute>
   <!-- Compose the invoker URL from the cluster node address -->
   <attribute name="InvokerURLPrefix">http://</attribute>
   <attribute name="InvokerURLSuffix">:82/invoker/JMXInvokerServlet</attribute>
   <attribute name="UseHostName">false</attribute>
   <attribute name="ExportedInterface">org.jnp.interfaces.Naming</attribute>
   <attribute name="JndiName"></attribute>
   <attribute name="ClientInterceptors">
      <interceptors>
         <interceptor>org.jboss.proxy.ClientMethodInterceptor</interceptor>
         <interceptor>org.jboss.proxy.SecurityInterceptor</interceptor>
         <interceptor>org.jboss.naming.interceptors.ExceptionInterceptor</interceptor>
         <interceptor>org.jboss.invocation.InvokerInterceptor</interceptor>
      </interceptors>
   </attribute>
</mbean>
```

5. 配置完后需要重启 JBOSS 服务才能生效

6. 防火墙配置

如防火墙关闭，则无需配置下面内容

vi /etc/sysconfig/iptables

编辑 iptables,加入新一行内容：-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 12345 -j ACCEPT

7. 查看配置及 JBOSS 服务是否启动成功

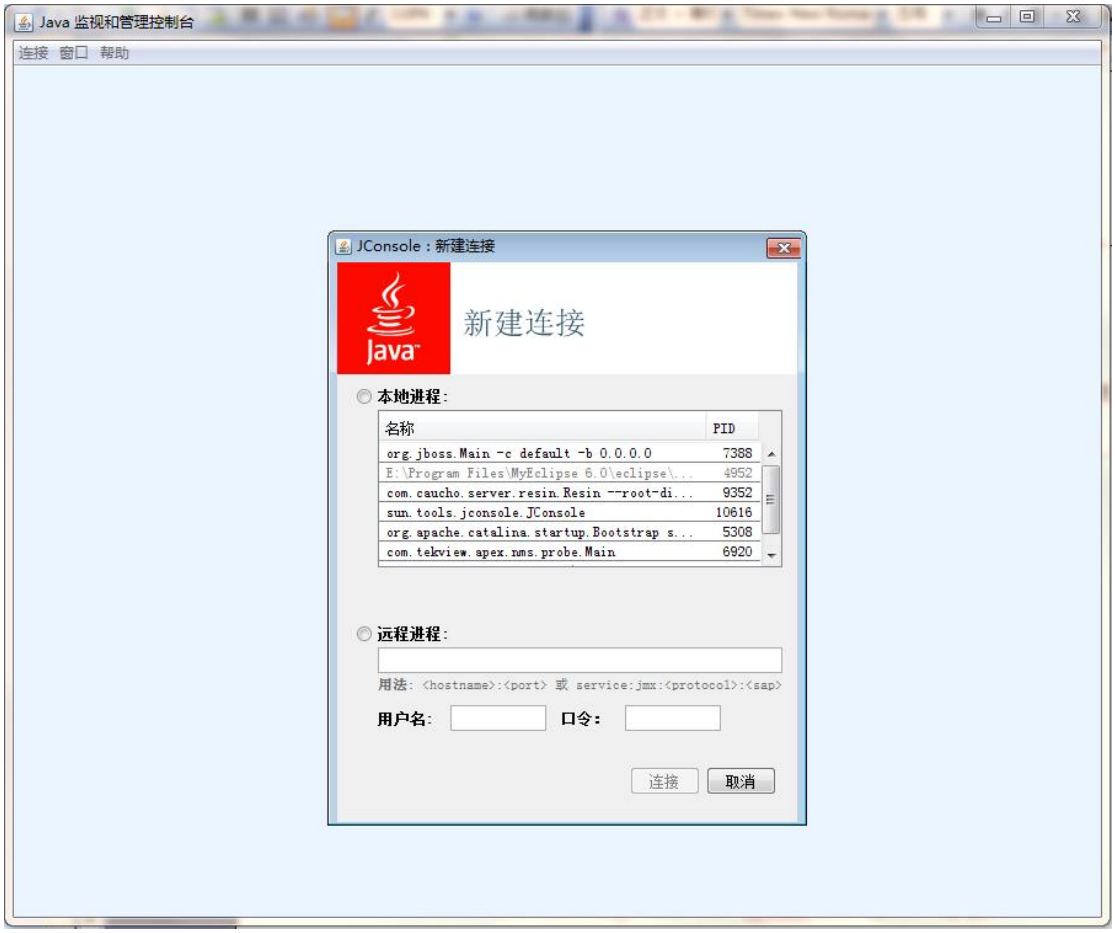
1). 用命令查看一下配置的端口和服务是否连通：

Netstat –an | grep 12345

2）JBOSS 成功启动后，可通过 JCONSLE 来查看刚才配置的参数是否成功

具本操作步骤如下：

a). 直接在命令行中键入 JCONSOLE 命令，会弹出下窗口界面：



b). 选择远程进程，输入 JBOSS 服务器所在 IP 及在上面配置的端口号，用户名和密码不用填。格式如下：

192.168.0.21:12345

c). 点击连接， 如果连接成功，说明配置正确。如连接不成功，则返回连接超时提示。

7. 注意事项

1）上所有参数需放在同一行，每一参数之间用空格隔开。

2）配置的端口不能已被占用。

18.2. JBoss 5.0.X/5.1.X

Windows 环境

1. 在启动脚本 RUN.BAT 中设置 JVM 启动参数：

```
set JAVA_OPTS=%JAVA_OPTS%
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=12345
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname= IP
```

注意：上参数应在放在同一行。

2. 将%JBOSS_HOME%\server\default\deploy\http-invoker.sar\META-INF\jboss-service.xml 文件中的所有 UseHostName 属性值改为 false,

或者在启动脚本 RUN.BAT 文件中 org.jboss.Main 后加上 JBOSS 所在机器的对外 IP 如：-b 192.168.0.97

3. 验证配置是否成功的方法与 JBOSS4.2.X 相同。

18.3. JBoss 6.0.X/6.1.X

Windows 环境

1. 在启动配置脚本 run.conf.bat 中设置 JVM 等启动参数：

1）set JAVA_OPTS=%JAVA_OPTS%
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=12345
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname= IP
注意：上参数应在放在同一行。

2） rem #Use the jboss logmanager
set "JAVA_OPTS=%JAVA_OPTS%
-Djava.util.logging.manager=org.jboss.logmanager.LogManager"
set "JAVA_OPTS=%JAVA_OPTS%
-Dorg.jboss.logging.Logger.pluginClass=org.jboss.logging.logmanager.LoggerPluginImpl"
pushd %DIRNAME%..
set "JBOSS_HOME=%cd%"
popd
set
"JBOSS_CLASSPATH=%JBOSS_CLASSPATH%;%JBOSS_HOME%\lib\jboss-logmanager.jar"

2. 在启动脚本 RUN.BAT 文件中 org.jboss.Main 后加上 JBOSS 所在机器的对外 IP 如：-b 192.168.0.97

3. 验证配置是否成功的方法与 JBOSS4.2.X 相同。

19. Resin

支持 resin3.0.X、resin4.0.X，Resin 的配置，不同的版本，不同的操作系统，配置各不相同。下面的配置说明只针 RESIN3.0 及 RESIN4.0

1. Linux 环境

1). RESIN3.0

a) 参数:

打开$RESIN_HOME/bin/wrapper.pl 文件，加入如下参数

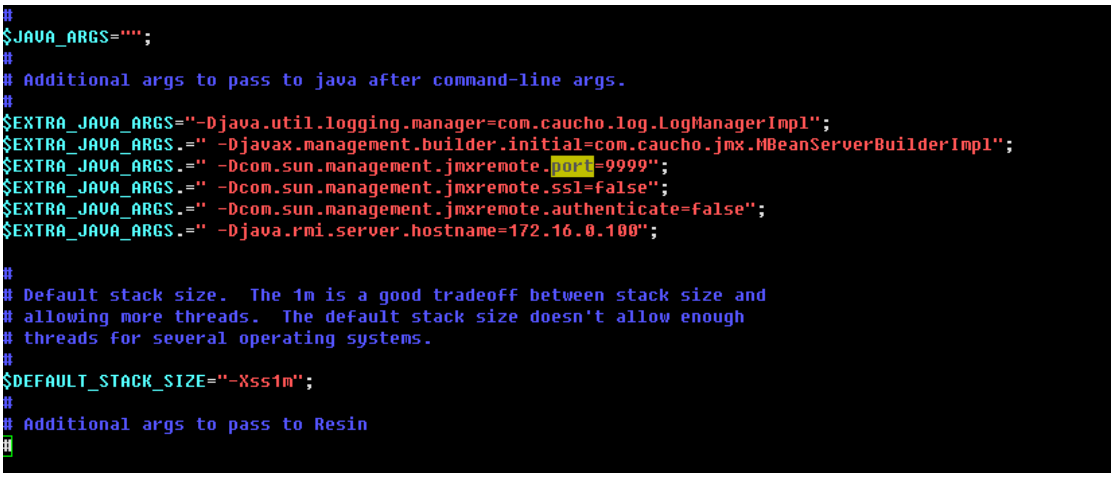
$EXTRA_JAVA_ARGS.=" -Dcom.sun.management.jmxremote.port=12345";

$EXTRA_JAVA_ARGS.=" -Dcom.sun.management.jmxremote.ssl=false";

$EXTRA_JAVA_ARGS.=" –Dcom.sun.management.jmxremote.authenticate=false";

$EXTRA_JAVA_ARGS.=" –Djava.rmi.server.hostname=hostIP";

b). 加入位置如下图：



2). RESIN4.0

a). 打开$RESIN_HOME\conf\resin.xml 文件， 在<server-default>标签内增加下列参数：

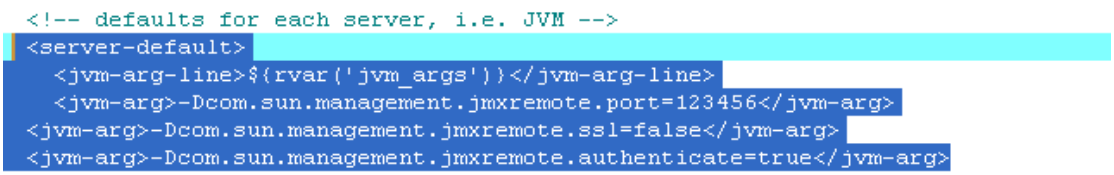
<jvm-arg>-Dcom.sun.management.jmxremote.port=123456</jvm-arg>

<jvm-arg>-Dcom.sun.management.jmxremote.ssl=false</jvm-arg>

<jvm-arg>-Dcom.sun.management.jmxremote.authenticate=false</jvm-arg>

<jvm-arg>-Djava.rmi.server.hostname=hostIP</jvm-arg>

b) 如下图



注意，如果在$RESIN_HOME\conf\local_jvm.xml 中配置了上参数，则无需再在resin.xml 文件中配置上参数，只需在$RESIN_HOME\conf\resin.xml 文件中打开下面这一行注释即可

#<resin:import path="${__DIR__}/local_jvm.xml"/>

2. Windows 环境

1）Resin3.0,打开%RESIN_HOME%\conf\resin.conf 文件，

2). Resin4.0 版本，打开%RESIN_HOME%\conf\resin.xml 文件

3). 加入参数及位置：

参数：

<jvm-arg>-Dcom.sun.management.jmxremote.port=123456</jvm-arg>
<jvm-arg>-Dcom.sun.management.jmxremote.ssl=false</jvm-arg>
<jvm-arg>-Dcom.sun.management.jmxremote.authenticate=false</jvm-arg>
<jvm-arg>-Djava.rmi.server.hostname=hostIP</jvm-arg>

b) 位置如下图

```
<!-- defaults for each server, i.e. JVM -->
<server-default>
  <jvm-arg-line>${rvar('jvm_args')}</jvm-arg-line>
  <jvm-arg>-Dcom.sun.management.jmxremote.port=123456</jvm-arg>
<jvm-arg>-Dcom.sun.management.jmxremote.ssl=false</jvm-arg>
<jvm-arg>-Dcom.sun.management.jmxremote.authenticate=true</jvm-arg>
```

3. 参数说明

1). 端口‘123456’可根据需要进行修改，且该端口就是在添加 RESIN 资源页面需要的 JMX 监听端口。

2). 参数 hostIP 即为 Tomcat 所在主机的 IP, 如果不配置这个参数，则有可能在添加被监控的资源是报 java.rmi.ConnectException: Connection refused to host: 错误。

4. 配置完后需要重启 RESIN 服务才能生效

1. 关闭防火墙配置

如防火墙关闭，则无需配置下面内容，

vi /etc/sysconfig/iptables

编辑 iptables,加入新一行内容：-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 12345 -j ACCEPT

2. 查看配置及 RESIN 启动是否成功

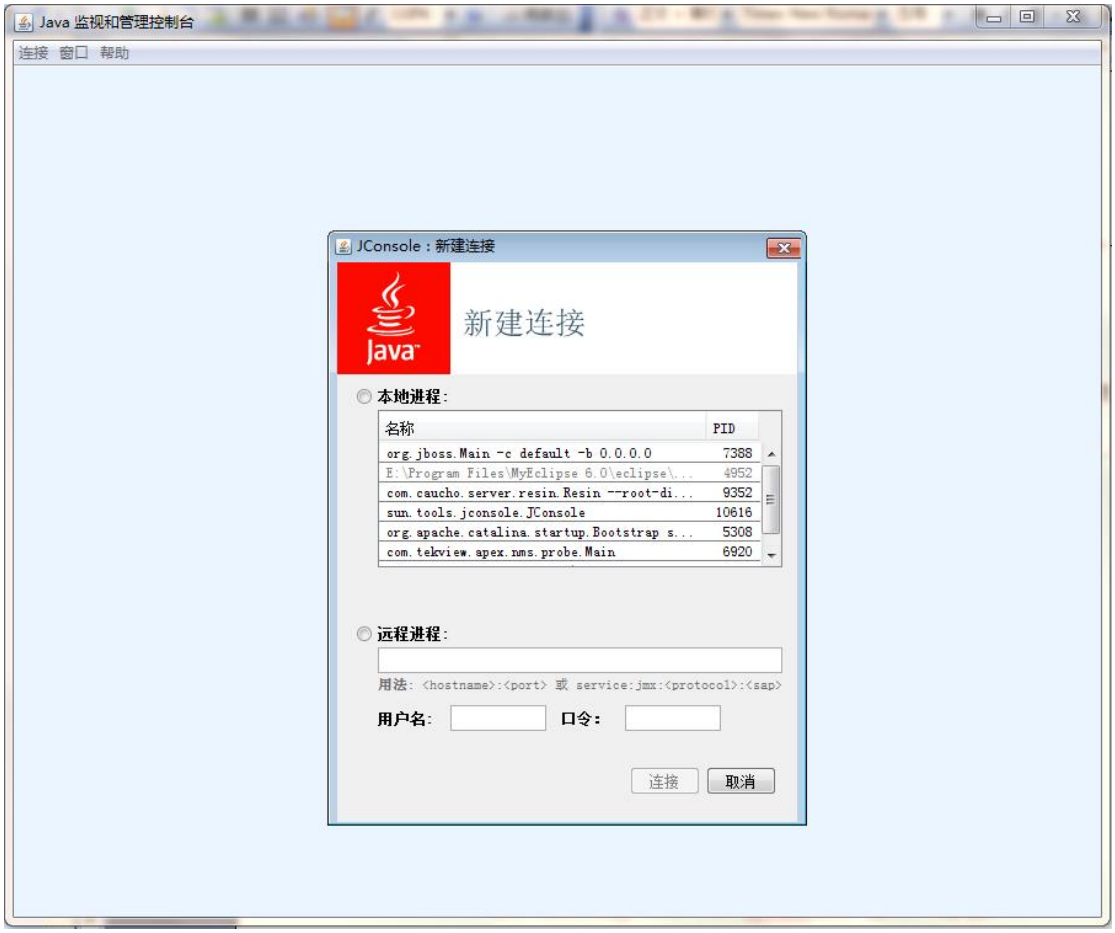
1）用命令查看一下配置的端口和服务是否连通：

Netstat –an | grep 12345

2）**RESIN** 成功启动后，可通过 JCONSLE 来查看刚才配置的参数是否成功

具本操作步骤如下：

a). 直接在命令行中键入 JCONSOLE 命令，会弹出下窗口界面：



b). 选择远程进程，输入 **RESIN** 服务器所在 IP 及在上面配置的端口号，用户名和密码不用填。格式如下：

192.168.0.21:12345

c). 点击连接， 如果连接成功，说明配置正确。如不成功，则返回连接超时提示。

5. 注意事项

1）上所有参数需放在同一行，每一参数之间用空格隔开。

2）配置的端口不能已被占用。

20. WebSphere

不支持采用集群模式部署的 WebSphere 监控。

登录 WebSphere 的集成解决方案控制台，进入安全性 --> 全局安全性 --> 去除“启用管理安全性”的勾选 --> 点击“应用” --> 保存到主配置 --> 重启 WAS

21. WebLogic

支持的 WebLogic 版本为 WebLogic8、WebLogic9、WebLogic10，不支持采用集群模式部署的 WebLogic 监控。

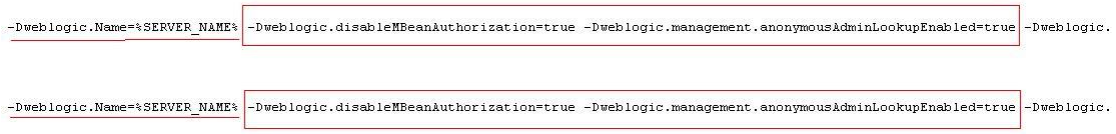
编辑 <WLS_HOME>/server/bin 目录下的 startWLS.cmdsh 文件，添加以下参数：
-Dweblogic.disableMBeanAuthorization=true
-Dweblogic.management.anonymousAdminLookupEnabled=true

重启 WebLogic 服务器，使配置生效。

如下图所示：

```
@rem Start Server

@echo off
if "%ADMIN_URL%" == "" goto runAdmin
@echo on
"%JAVA_HOME%\bin\java" %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS% -Dweblogic.Name=%SERVER_NAME%
goto finish

:runAdmin
@echo on
"%JAVA_HOME%\bin\java" %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS% -Dweblogic.Name=%SERVER_NAME%

:finish

ENDLOCAL
```

在下划线所示的后面加上框选的配置



startWLS.cmd/sh 示例文件:（**黑体部分就是要配置的参数**）

"%JAVA_HOME%\bin\java" %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS% -classpath
"%CLASSPATH%" -Dweblogic.Name=%SERVER_NAME%
-Dbea.home="C:\WebLogic\WL7.0" **-Dweblogic.disableMBeanAuthorization=true**
-Dweblogic.management.anonymousAdminLookupEnabled=true
-Dweblogic.management.username=%WLS_USER%
-Dweblogic.management.password=%WLS_PW%
-Dweblogic.management.server=%ADMIN_URL%
-Dweblogic.ProductionModeEnabled=%STARTMODE%
-Djava.security.policy="%WL_HOME%\server\lib\weblogic.policy" weblogic.Server
goto finish

:runAdmin
@echo on
"%JAVA_HOME%\bin\java" %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS% -classpath
"%CLASSPATH%" -Dweblogic.Name=%SERVER_NAME%
-Dbea.home="C:\WebLogic\WL7.0" **-Dweblogic.disableMBeanAuthorization=true**
-Dweblogic.management.anonymousAdminLookupEnabled=true
-Dweblogic.management.username=%WLS_USER%
-Dweblogic.management.password=%WLS_PW%
-Dweblogic.ProductionModeEnabled=%STARTMODE%
-Djava.security.policy="%WL_HOME%\server\lib\weblogic.policy" weblogic.Server

注意事项

以上参数需放在同一行，每个参数之间用空格隔开。

22. Apache Http 服务器

支持 Apache2.2

1. 对 Apache Web 服务器的监控，打开%APCHE_HOME%\conf\httpd.conf 文件，在该文件中加入下列配置：

<Location /server-status>
SetHandler server-status
Order deny,allow
Allow from all
</Location>
ExtendedStatus On

2. 加入位置如下图：

```
#LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule version_module modules/mod_version.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so

<Location /server-status>
  SetHandler server-status
  Order deny,allow
  Allow from all
</Location>
ExtendedStatus On

<IfModule !mpm_netware_module>
<IfModule !mpm_winnt_module>
#
```

3. 并且找到 LoadModule status_module modules/mod_status.so 这一行，把注释打开，
4. 重启 apache 服务器就可以了。

23. 网络服务/系统服务

任何基于 TCP/UDP 提供网络服务或系统服务的进程，均可以进行监控，这些网络服务一般是长时间运行在 Windows/Linux/Unix/交换机/路由器上的进程或系统服务，对外提供某种应用功能，比如 DHCP、TFTP、FTP 服务、邮件服务等等。

输入网络服务的 IP 地址，监听端口和连接超时时间并确定网络服务是基于 TCP 还是基于 UDP 协议，按照提示输入以上参数即可对网络服务进行监控。

24. URL 监控

URL 监控也称网页监控，通过模拟浏览器请求某个网页来判断网络或企业 WEB 应用工作是否正常。

1. 确定要监控的网页的完整 URL
2. 支持 GET/POST 两种方式提交 HTTP 请求参数，参数的格式为 key=value，如果有多个参数，请用英文格式的分号（;）隔开
3. 如果要监控的网页需要登录验证后才能访问，请输入登录的 URL 地址、用户名和密码
4. 用户名和密码，不同的应用系统的 HTML 字段名称是不一样的，请根据实际情况填写（可通过查看登录页面的 HTML 源代码来获取用户名和密码字段的 HTML 输入框名

称），格式为 key=value。

25. MySQL 数据库

支持 Mysql5.0.x，Mysql5.1.x，Mysql5.5.x

对 MYSQL 这类数据库资源的监控，登陆账号不必具有 DBA 角色，只需要用具有 DBA 角色的用户登录到 MYSQL 数据库操作系统，创建一个新的用户，赋给该用户某些有限的角色、权限即可。

针对目前版本对 MYSQL 资源的监控，只需用户具有对所有数据库、所有表具有查询功能即可。所以只需做如下操作设置：

1) 创建用户

CREATE USER 'test'@'%' IDENTIFIED BY '123456'

2) 分配权限

GRANT SELECT ON *.* TO 'test'@'%'

其中: test 为用户名, %代表任何远程 IP 都可以访问, 123456 是密码

第一个*代表所有数据库，第二个*代表数据库中的所有表.

26. Oracle 数据库

不支持 RAC 模式部署下的 Oracle 数据库监控。

支持的 Oracle 数据库版本为 Oracle9i、10g、11g，与 MYSQL 类似，对 Oracle 数据库监控，账号无需具备 DBA 角色，请使用 DBA 角色的用户登录到 ORACLE，执行如下操作：

- 基于表空间创建用户帐号

```
CREATE USER "APPTEST" IDENTIFIED BY VALUES '3C611F58B66FD7C1'
 DEFAULT TABLESPACE TEKVIEW_DATA
 TEMPORARY TABLESPACE TEKVIEW_TEMP
 PROFILE DEFAULT;
```

- 为用户分配相应的角色权限

```
GRANT UNLIMITED TABLESPACE TO "APPTEST";
GRANT CONNECT TO "APPTEST";
GRANT RESOURCE TO "APPTEST";
GRANT SELECT_CATALOG_ROLE TO "APPTEST";
ALTER USER "APPTEST" DEFAULT ROLE CONNECT,
SELECT_CATALOG_ROLE;
ALTER USER "APPTEST" QUOTA Unlimited ON TEKVIEW_DATA;
```

注意，标蓝色部分的 APPTEST 是用户名，3C611F58B66FD7C1 是密码，TEKVIEW_DATA TEKVIEW_TEMP 是表空间和临时表空间的名称，请根据实际情况自行设定。

27. DB2 数据库

通过 JDBC 连接 DB2 数据库，从系统管理相关表中获取数据库性能数据，支持的 DB2 版本为：

DB2 8.1
DB2 9.7

28. SQL Server 数据库

支持的 SQLSERVER 数据库版本为： SQLServer2000、2005、SQLServer2008

SQLSERVER 添加时目前只支持 SQL 认证方式。用户需要具有读取 SQLSERVER 系统表，系统视图、系统存储过程及创建临时表的角色和权限。 因为 SQLSERVER 被监控指标的数据都是通过 SQL 语句去系统表、系统视图表获取得到的。

29. Informix 数据库

通过 JDBC 协议连接到 Informix 数据库， 从系统管理表中查询数据库的相关性能指标。

30. AIX 服务器

支持通过 Telnet/SSH2/SNMP 三种方式对 AIX 服务器监控，请按下述步骤实现对 AIX 服务器的监控：

1) 打开 AIX 服务器的 Telnet/SSH 服务，确保通过客户端工具（如 putty）可以通过用户名和口令访问目标 AIX 服务器

2) 进入【资源管理】列表，点击“添加”按钮，输入 AIX 服务器的 IP 地址、用户名、密码、轮询周期等数据，将 AIX 服务器添加到系统中，等待至少一个轮询周期后通过 AIX 服务器的明细界面。

31. SCO Unix 服务器

通过 SSH2 协议对 SCO Unix 服务器进行监控，SCO UNIX 主要包括 SCO Openserver 和 Sco Unixware 两种类型。它们都是 UNIX 产品线的一个分支，即由 UNIX 演化而来，其中 SCO Openserver 是一套免费开源的 UNIX 操作系统，而 SCO Unixware 是一套商业的 UNIX 操作

系统， 目前支持的版本为：

SCO OPENSERVER 6.0.0
SCO UNIXWARE7.1.4.

32. Solaris 服务器

支持通过 SSH2 协议对 Solaris 服务器监控，当前支持的 Solaris 版本为：

Solaris9
Solaris10

请按照下述步骤实现对 Solaris 服务器的监控：

1) 打开 Solaris 服务器的 SSH 服务，确保通过 SSH 客户端工具（如 putty）可以通过用户名和口令访问目标 Solaris 服务器

2) 进入【资源管理】列表，点击“添加”按钮，输入 Solaris 服务器的 IP 地址、用户名、密码、轮询周期等数据，将 Solaris 服务器添加到系统中，等待至少一个轮询周期后通过 Solaris 服务器的明细界面，可以查看 Solaris 服务器的各项指标数据。

33. Linux 服务器

可通过 SSH2/SNMP 协议对 Linux 服务器进行监控，支持的 Linux 发行版为：

RedHat Enterprise Linux 5.x、6.x
CentOS 5.x、6.x
Oracle Enterprise Linux 5.x
OpenSUSE 12.3
SUSE Linux Enterprise Server 11
Ubuntu Linux 9.0.4

其它 Linux 发行版本可能存在命令上的兼容性差异而导致某些性能指标获取失败。

通过 SSH2 方式对服务器进行监控，请确保使用的监控账号具备较高的操作系统权限，否则可能会导致某些命令由于不具备相应的操作系统权限，从而执行失败无法获取某些指标的数据。

34. Windows 服务器

可通过 WMI/SNMP 协议对 Windows 服务器进行监控，支持的 Windows 服务器操作系统版本为：

Windows Server 2000
Windows Server 2003
Windows Server2003 R2
Windows Server 2008
Windows Server 2008 R2

34.1. SNMP 方式监控

首先安装 Windows 操作系统自带的 SNMP Agent 组件，并配置好 SNMP 读共同体、写共同体（可选），并启动 SNMP 系统服务。

34.2. WMI 方式监控

WMI(Windows Management Instrumentation)即 Windows 管理规范，是一项核心的 Windows 管理技术；用户可以使用 WMI 管理本地和远程计算机。WMI 中的“Instrumentation”特指 WMI 可以获得关于计算机内部状态的信息，这与汽车仪表盘获得并显示引擎的状态信息非常类似。WMI 对磁盘、进程、和其他 Windows 系统对象进行建模，从而实现“指示”功能。这些计算机系统对象采用类来建立模型，例如 **Win32_LogicalDisk** 或 **Win32_Process**；如您所料，Win32_LogicalDisk 类用于建立在计算机上安装的逻辑磁盘的模型，Win32_Process 类用于建立正在计算机上运行的任何进程的模型。这些类基于一个名为通用信息模型（Common Information Model，CIM）的可扩展架构。CIM 架构是分布式管理任务组（Distributed Management Task Force）的一个公开标准。WMI 官方文档：http://msdn2.microsoft.com/en-us/library/aa394582.aspx

34.3. 远程使用 WMI

WMI 使用 DCOM 来实现远程通信，而 DCOM 是建立在 RPC（Remote Procedure Call，远程过程调用）协议之上的。DCOM（Distributed Component Object Model）即分布式组件对象模型，是一系列微软的概念和程序接口，利用这个接口，客户端程序对象能够请求来自网络中另一台计算机上的服务器程序对象。

DCOM 基于组件对象模型（COM），COM 提供了一套允许同一台计算机上的客户端和服务器之间进行通信的接口。DCOM 是 COM 的扩展，它支持不同的两台机器上的组件间的通信，而且不论它们是运行在局域网、广域网、还是 Internet 上。借助 DCOM 你的应用程序将能够任意进

行空间分布。

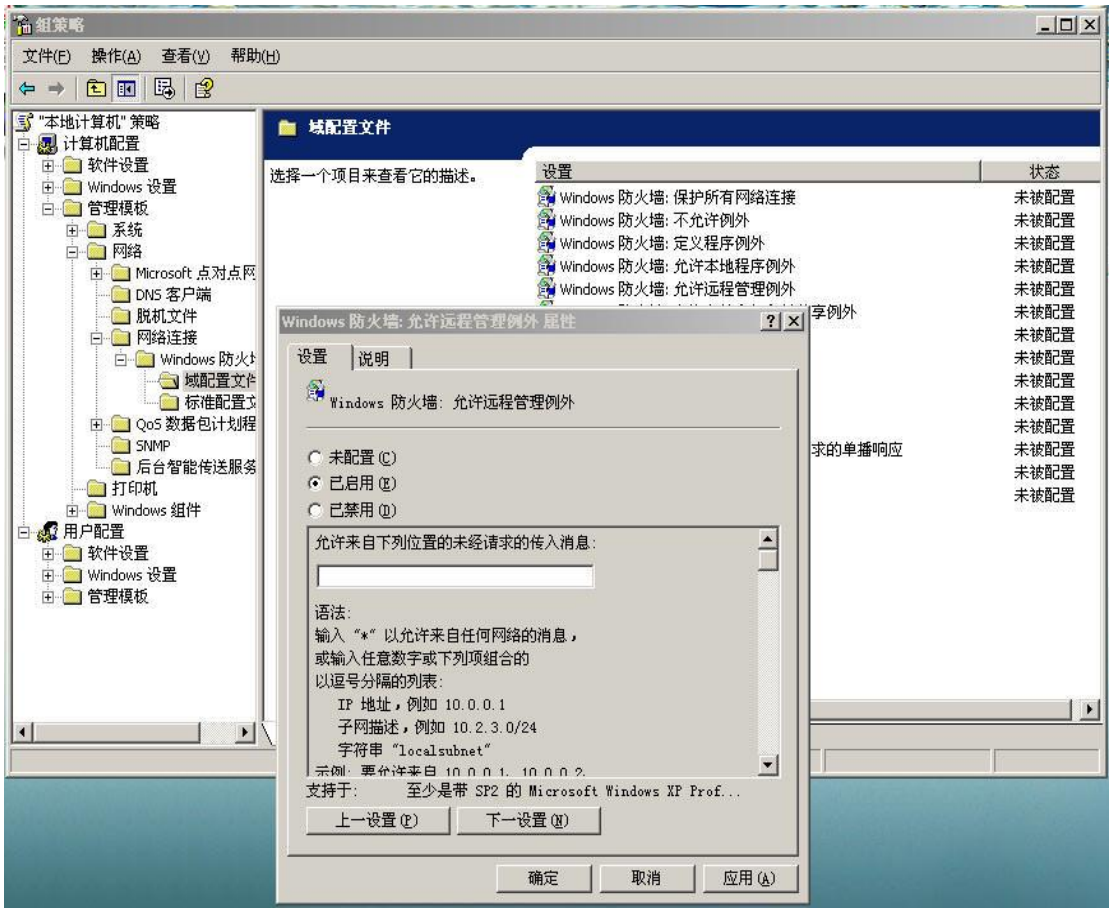
为了使得远程的 Windows 服务器能够被基于 WMI 技术的客户端程序（在这里是 APEX IT 综合管理系统）所管理，需要在远程服务器上进行正确的配置，否则会造成监控失败，请按照下面的章节逐项进行设置，当遇到问题时注意仔细核对步骤，不要有遗漏。

34.4. Windows 系统自带防火墙设置

使用 WMI 监控远程机器时，会首先访问远程的 RPC 服务器，而防火墙会屏蔽 RPC 端口（135 端口），导致出现“RPC 服务器不可用”错误，解决该问题最简单的办法就是直接关闭防火墙，也许有的人不愿意关闭防火墙，那么我们也可以对防火墙进行设置，下面我就介绍怎样设置 windows 系统自带的防火墙。

设置步骤：

- 单击“开始”，单击“运行”，键入“gpedit.msc” 然后单击“确定”
- 依次展开“计算机配置”，“管理模板”，“网络”，“网络连接”，“windows 防火墙”，“域配置文件”
- 右键单击“Windows 防火墙：允许远程管理例外”，然后单击“属性”
- 单击“已启用”，然后单击“确定”



图：设置 windows 系统自带防火墙

如果你嫌上面的步骤太繁琐，也可以用下面的命令来代替，可以起到同样的效果：

```
netsh firewall set service RemoteAdmin enable
```

注：Window 系统自带防火墙如果不允许远程管理例外或关闭，则会导致添加 Windows 监控报“RPC 服务器不可用”的错误。

34.5. Windows 系统服务设置

远程计算机上必须要启动的 Windows 服务（保证所有远程访问和 WMI 相关服务启用并运行）：

COM+ Event System
Remote Access Auto Connection Manager
Remote Access Connection Manager
Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locator
Remote Registry
Server

Windows Management Instrumentation

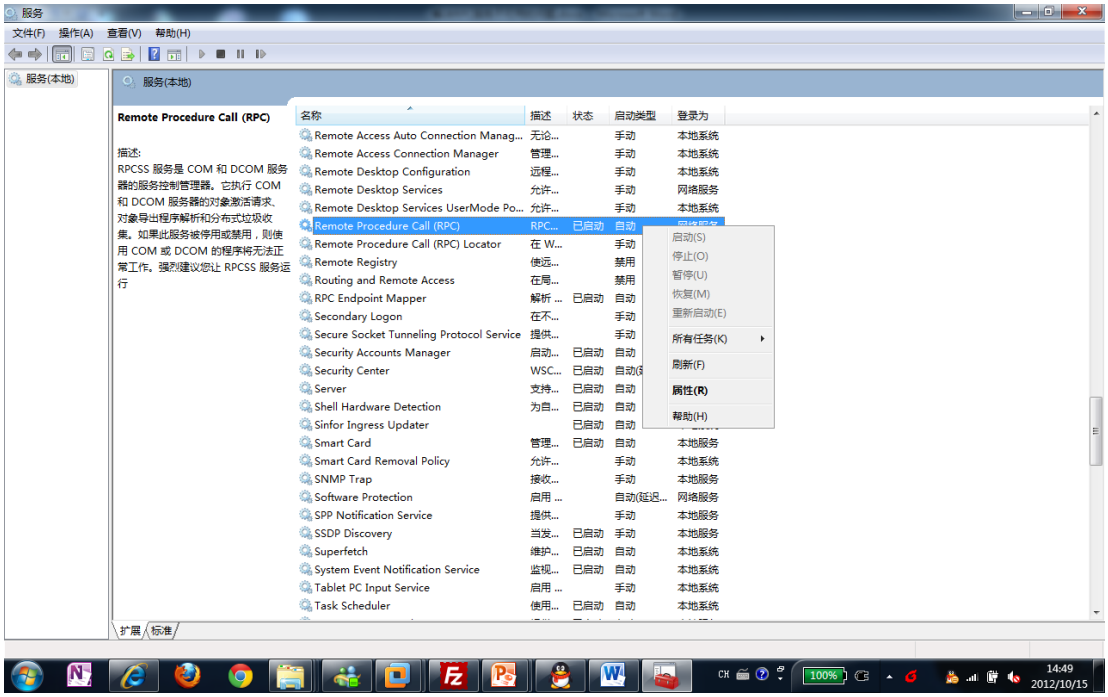
Windows Management Instrumentation Driver Extensions

WMI Performance Adapter

Workstation

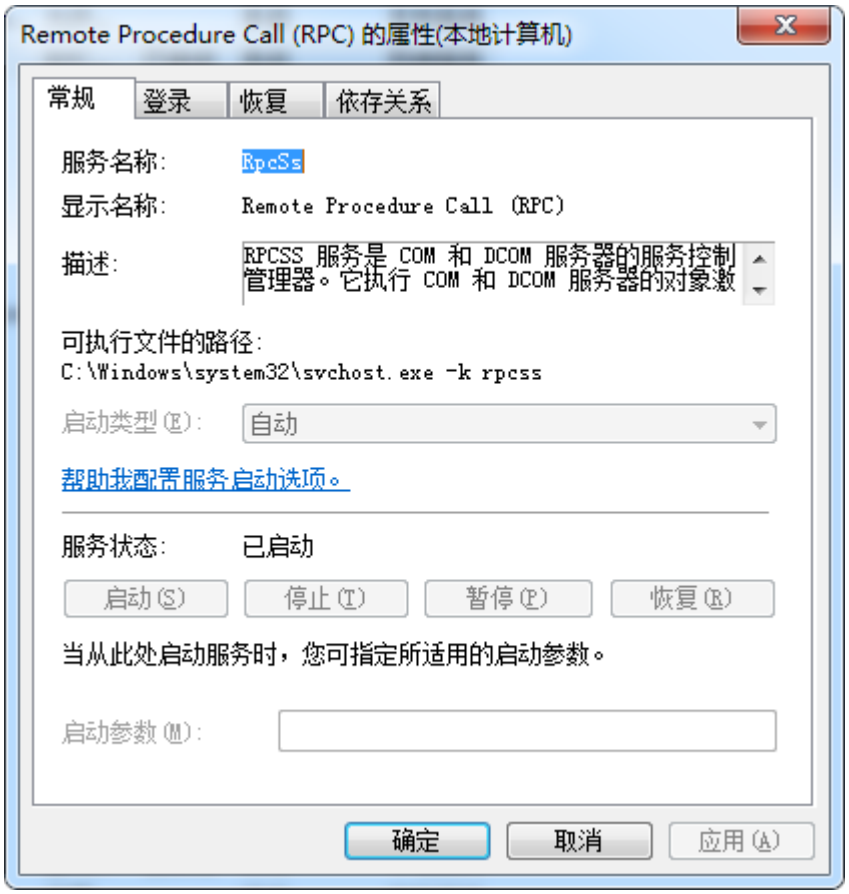
按上述操作设置后如果添加 Windows 监控仍然报“RPC 服务器不可用”的错误，还需做如下设置：

■ 检查 RPC 服务属性状态，如下图所示：

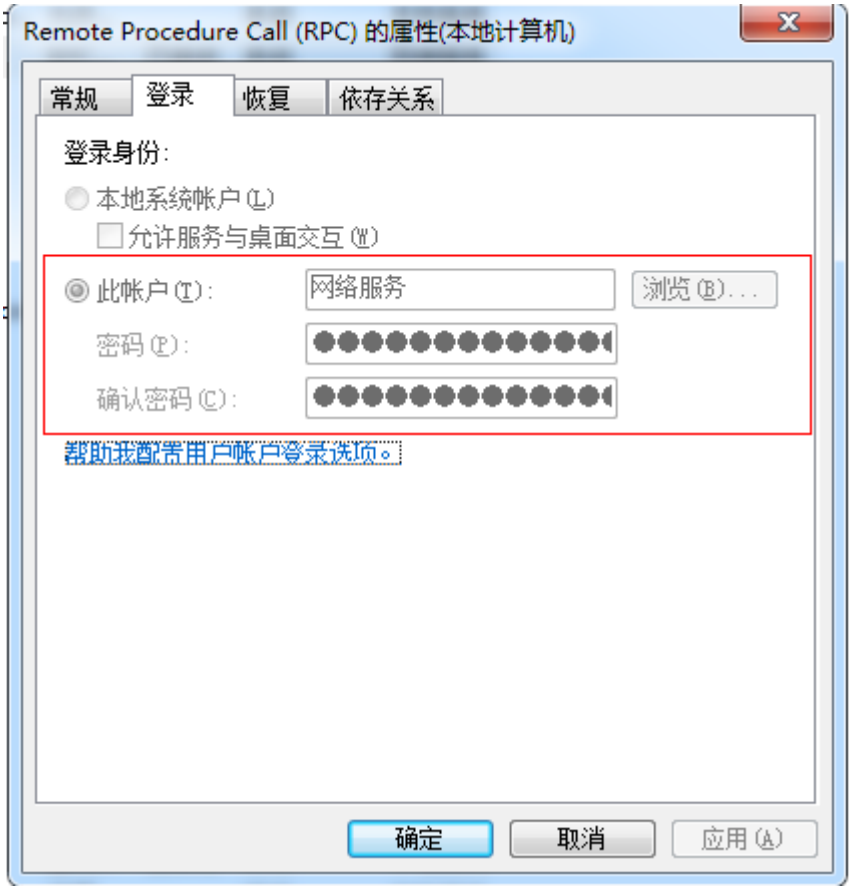


在 RPC 服务上右键，看到启动、停止、重新启动等按钮是灰色，不可操作的状态。

■ 右键查看 RPC 服务的属性，如下图所示：



点击登录页签，如下图所示：



修改登录身份，选择本地系统账户，保存后退出。

■ 使用 WMI 修复工具修复 WMI 服务

将下列内容保存为 bat 文件，命名为：FIXWMI.bat

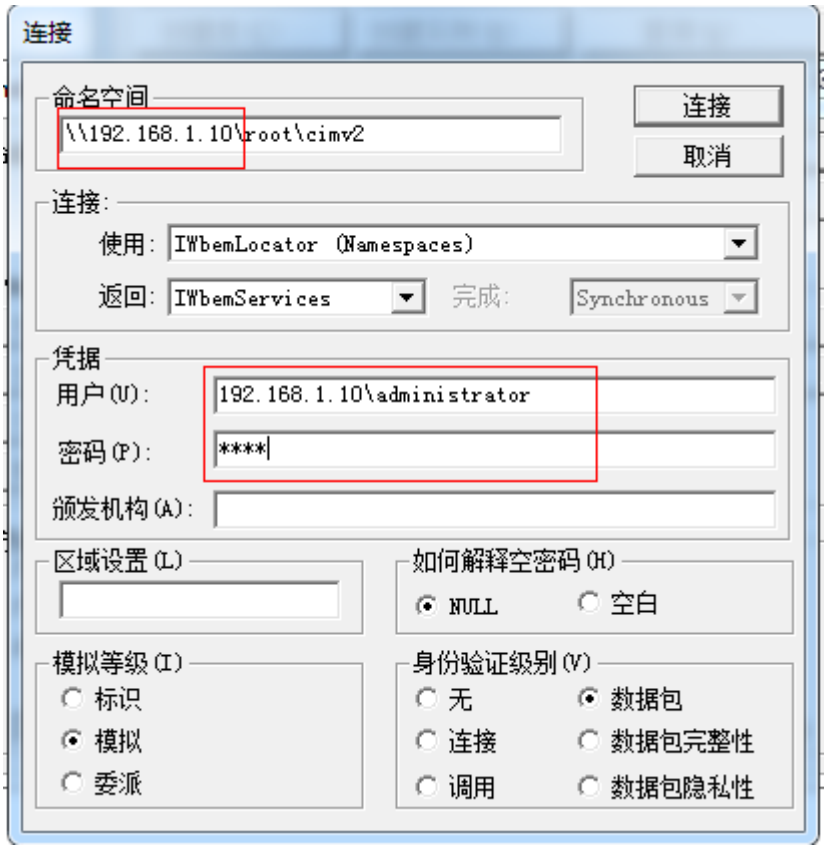
```
@echo on
cd /d c:\temp
if not exist %windir%\system32\wbem goto TryInstall
cd /d %windir%\system32\wbem
net stop winmgmt
winmgmt /kill
if exist Rep_bak rd Rep_bak /s /q
rename Repository Rep_bak
for %%i in (*.dll) do RegSvr32 -s %%i
for %%i in (*.exe) do call :FixSrv %%i
for %%i in (*.mof,*.mfl) do Mofcomp %%i
net start winmgmt
goto End

:FixSrv
if /I (%1) == (wbemcntl.exe) goto SkipSrv
if /I (%1) == (wbemtest.exe) goto SkipSrv
if /I (%1) == (mofcomp.exe) goto SkipSrv
%1 /RegServer

:SkipSrv
goto End

:TryInstall
if not exist wmicore.exe goto End
wmicore /s
net start winmgmt
:End
```

将 FIXWMI.bat 文件放到目标服务器的任一目录下，双击运行。

■ 验证 WMI 命名空间能够正常访问

在本地 PC 机上，运行-wbemtest，打开 WMI 连接测试工具，如下图所示：

点击“连接”，如下图所示：

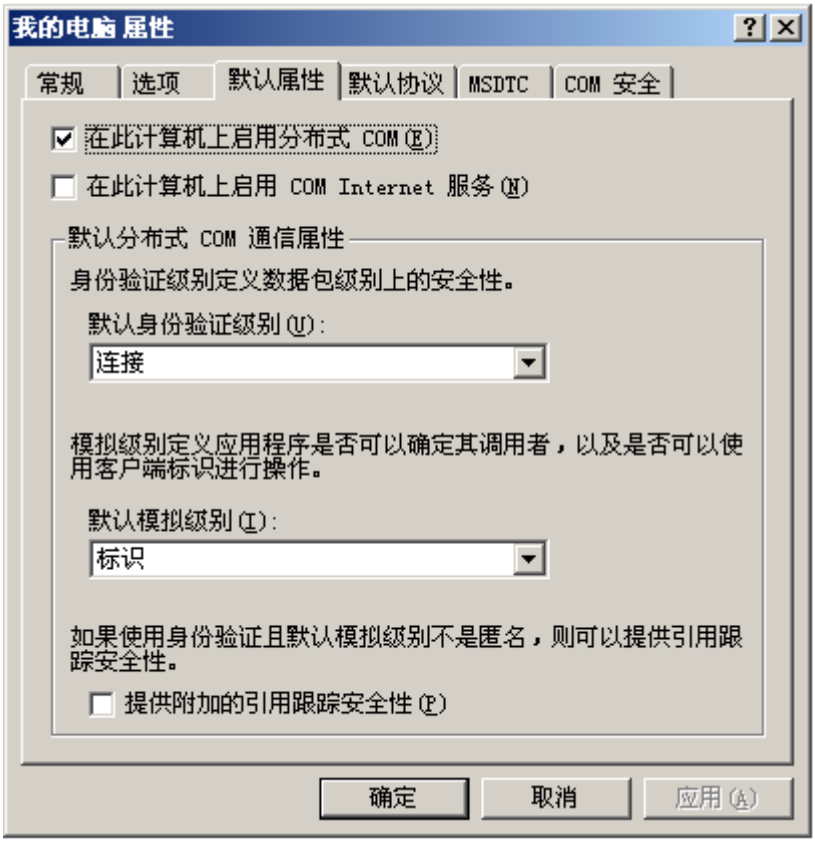


输入红色方框的内容，点击“连接”，测试 WMI 是否可以正常访问，如果可以，请到监控系统添加该服务器资源。

34.6. DCOM 设置

34.6.1. 启用分布式 COM

a) 单击“开始”，单击“运行”，键入 dcomcnfg，然后单击“确定”；
b) 依次展开“组件服务”、“计算机”，然后展开“我的电脑”，右键单击“我的电脑”，然后单击“属性”；
c) 在“我的电脑”对话框中，单击“默认属性”选项卡，
d) 选中“在此计算机上启用分布式 COM”；
e) 选择“默认身份验证级别”为“连接”；
f) 选择“默认模拟级别”为” 标识”；



g) 在“我的电脑”对话框中，单击“默认协议”选项卡，选中“面向连接的 TCP/IP”。

34.6.2. 用户权限设置

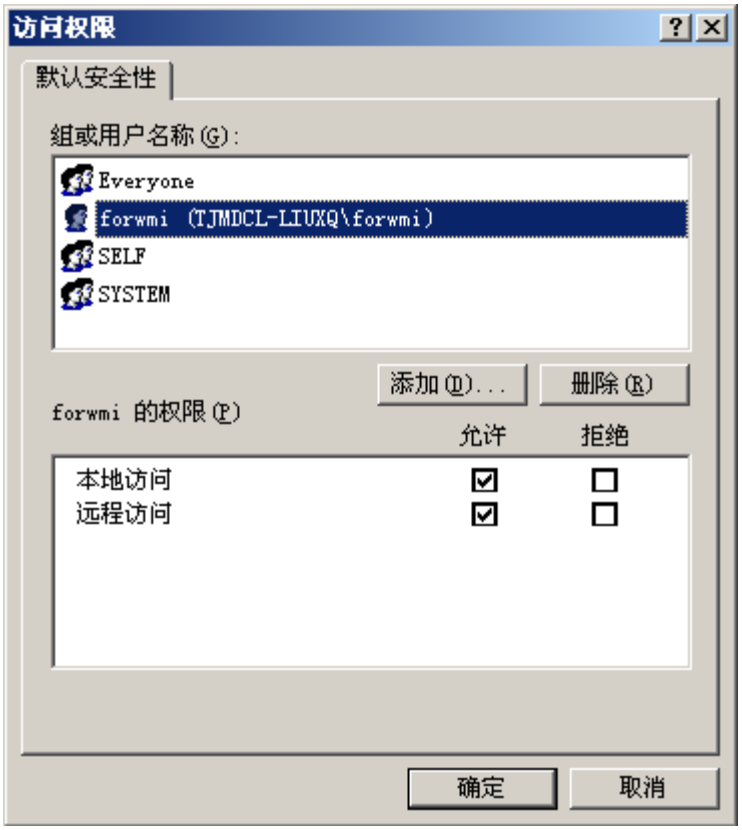
a) 单击“开始”，单击“运行”，键入 dcomcnfg，然后单击“确定”；
b) 依次展开“组件服务”、“计算机”，然后展开“我的电脑”，右键单击“我的电脑”，然后单击“属性”；

c) 在“我的电脑”对话框中，单击“COM 安全”选项卡；

d) 在“访问权限”下，单击“编辑限制”按钮；

e) 在“访问权限”对话框中，如果用户 forwmi 没有在“组或用户名称”列表中，请按照下列步骤操作：

1. 在“访问权限”对话框中，单击“添加”
2. 在“选择用户、计算机或组”对话框中，将用户 forwmi 添加到“输入对象名称来选择”框中，然后单击“确定”
3. 在“访问权限”对话框中，在“组或用户名称”框内选择您的用户和组。在“用户权限”下的“允许”栏中，选择“远程访问”，然后单击“确定”



f) 在“启动和激活权限”下，单击“编辑限制”按钮；

g) 重复步骤(e)，把 forwmi 用户添加“远程启动”和“远程激活”权限，如下图所示。

34.7. 域账号作为监控用户时的设置

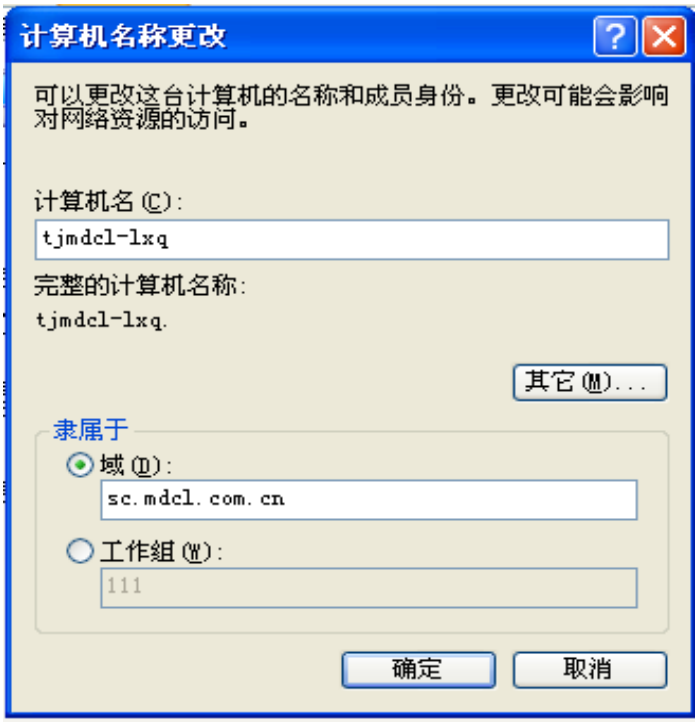
使用域账号作为监控用户还需做如下设置。

1) 把被监控端机器加入域

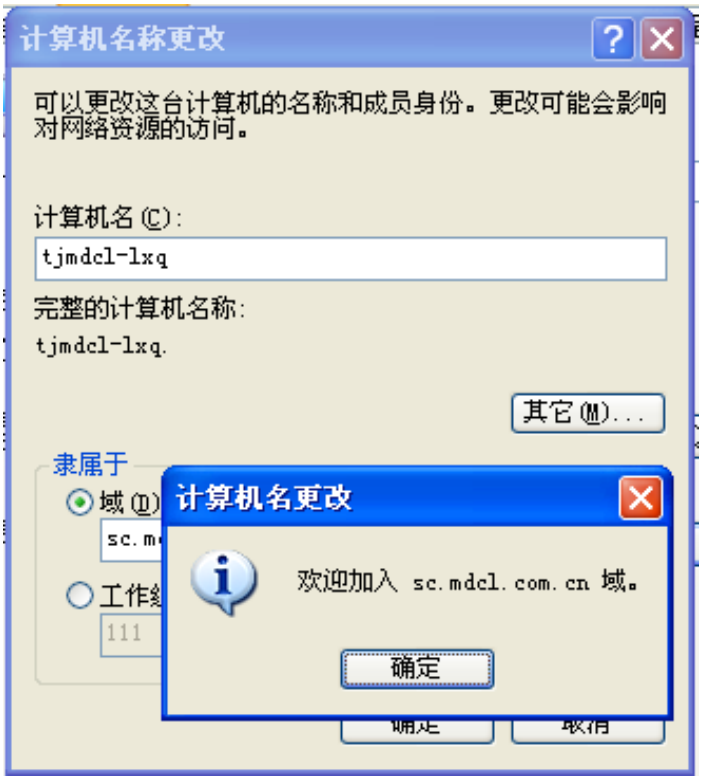
假如使用域账号，比如：“sc\bsmtest”来监控公司所有的机器，使用域账号只能监控域中的机器，如果被监控端机器不在域中，则需要把其加到域中。下面介绍加入域的步骤：

a) 在桌面上右键点击“我的电脑”，选择“属性”，在弹出的对话框中选择“计算机名”选项卡；然后选择“要重新命名此计算机或加入域，单击更改”字符串右面的“更改”按钮；

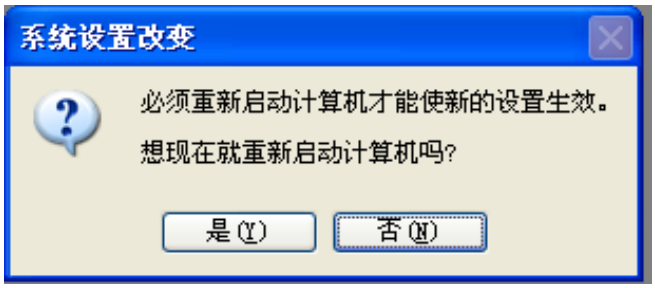
b) 在弹出的对话框中，选择“域”单选框，在域名编辑框中输入域的名称，在这里域名是“sc.mdcl.com.cn”，然后点击“确定”按钮；



如果弹出类似下面的对话框，则表示进入域成功：



c) 依次点击“确定”按钮，退出设置，最后会弹出一个重启机器的对话框，选择“是”，这样重新启动机器之后，就可以了。

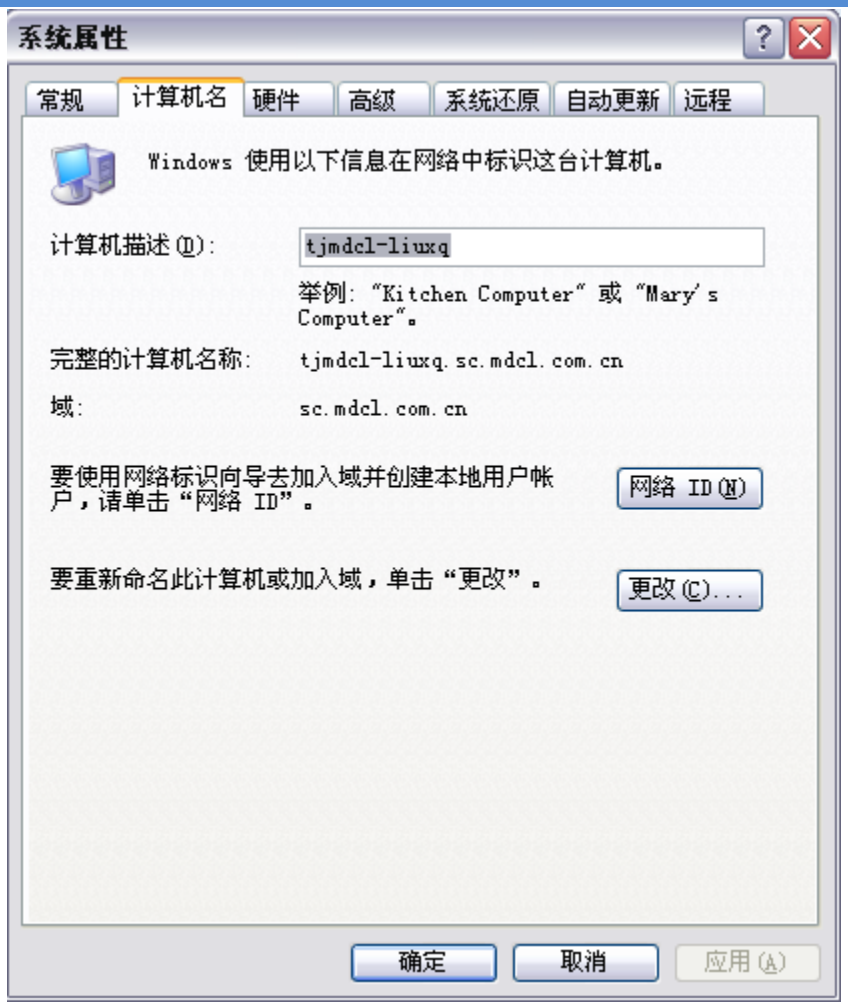


2) 把被监控机器退出域，然后重新加入域

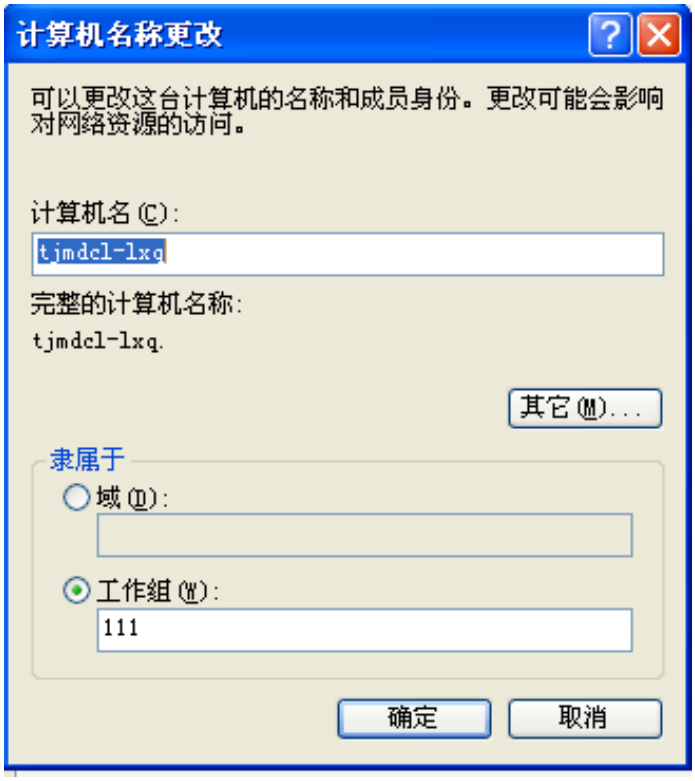
如果被监控端机器在域中，则需要先把机器退出域，然后重新加入域，才可以。我们先介绍怎样退出域和重新加入域，然后再进行详细解释。

a) 退出域，然后重新加入域的步骤

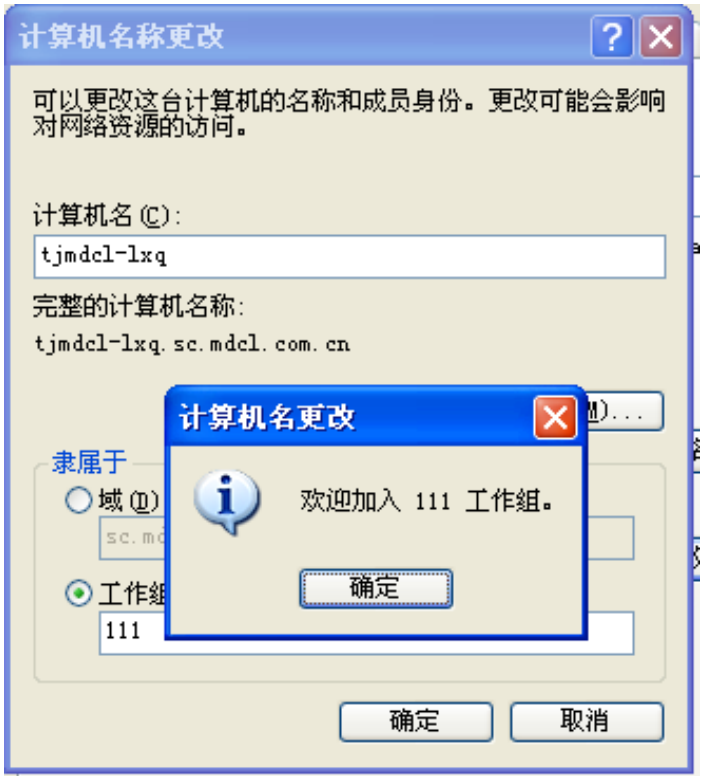
(1) 在桌面上右键点击“我的电脑”，选择“属性”，在弹出的对话框中选择“计算机名”选项卡；然后选择“要重新命名此计算机或加入域，单击更改”字符串右面的“更改”按钮；



(2) 在弹出的对话框中，选择“工作组”单选框，在工作组名称编辑框中随便输入一个字符串即可，例如我输入的是字符串“111”，然后点击“确定”按钮；



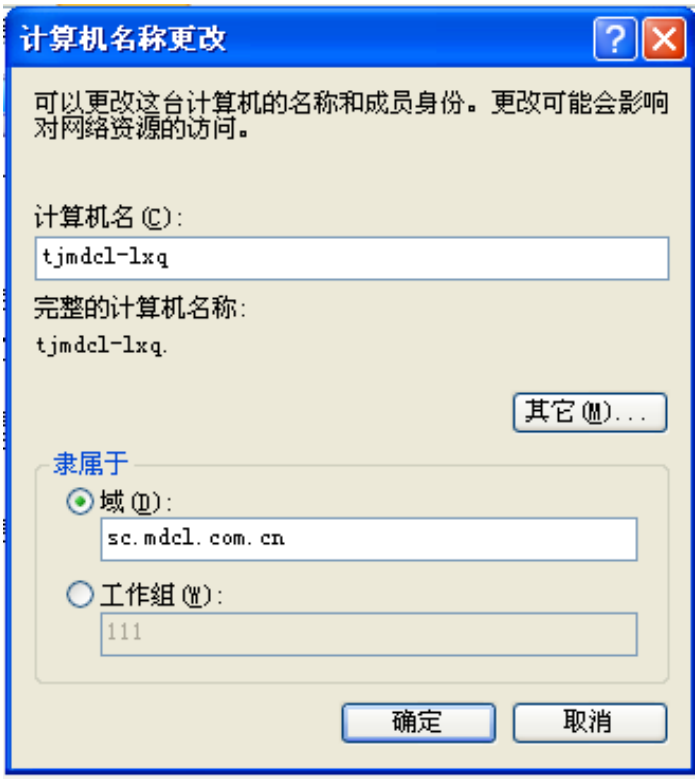
如果退出域成功，则会弹出类似下面的对话框：



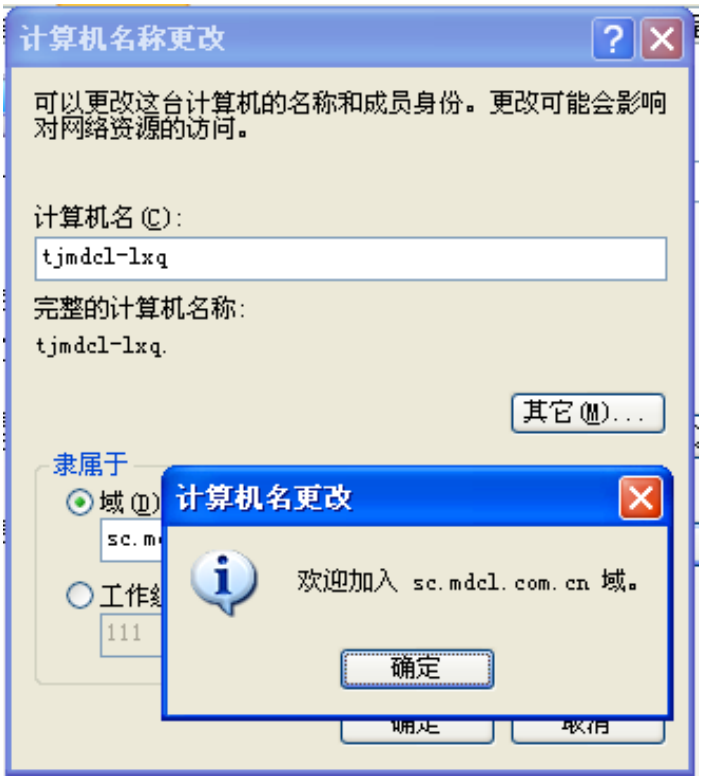
(3) 依次点击“确定”按钮，退出设置，然后重新启动计算机；

(4) 当计算机重新启动之后，需要再次在桌面上右键点击“我的电脑”，选择“属性”，选择“计算机名”选项卡；然后再点击“更改”按钮；

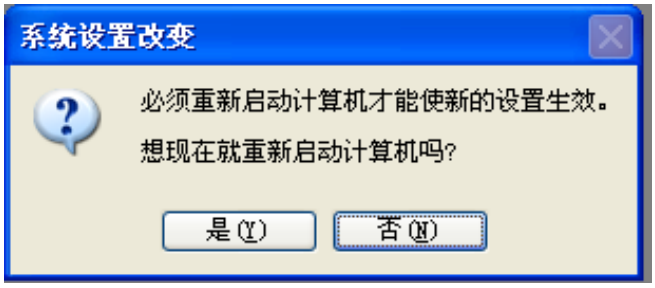
(5) 在弹出的对话框中，选择“域”单选框，在域名编辑框中输入域的名称，在这里域名是“sc.mdcl.com.cn”，然后点击“确定”按钮；



如果弹出类似下面的对话框，则表示进入域成功：



(6) 依次点击“确定”按钮，退出设置，最后会弹出一个重启机器的对话框，选择“是”，这样重新启动机器之后，就可以了。



b) 原因解释

（1）加入过域但机器的域信息已经出现问题

原因：因被监控端需要使用域进行登录验证，但该监控端本身从域控制器上获取并保存在的信息已经损坏或丢失，无法从域控制器上验证登录用户的有效性，因而无法被 MARA 监控到

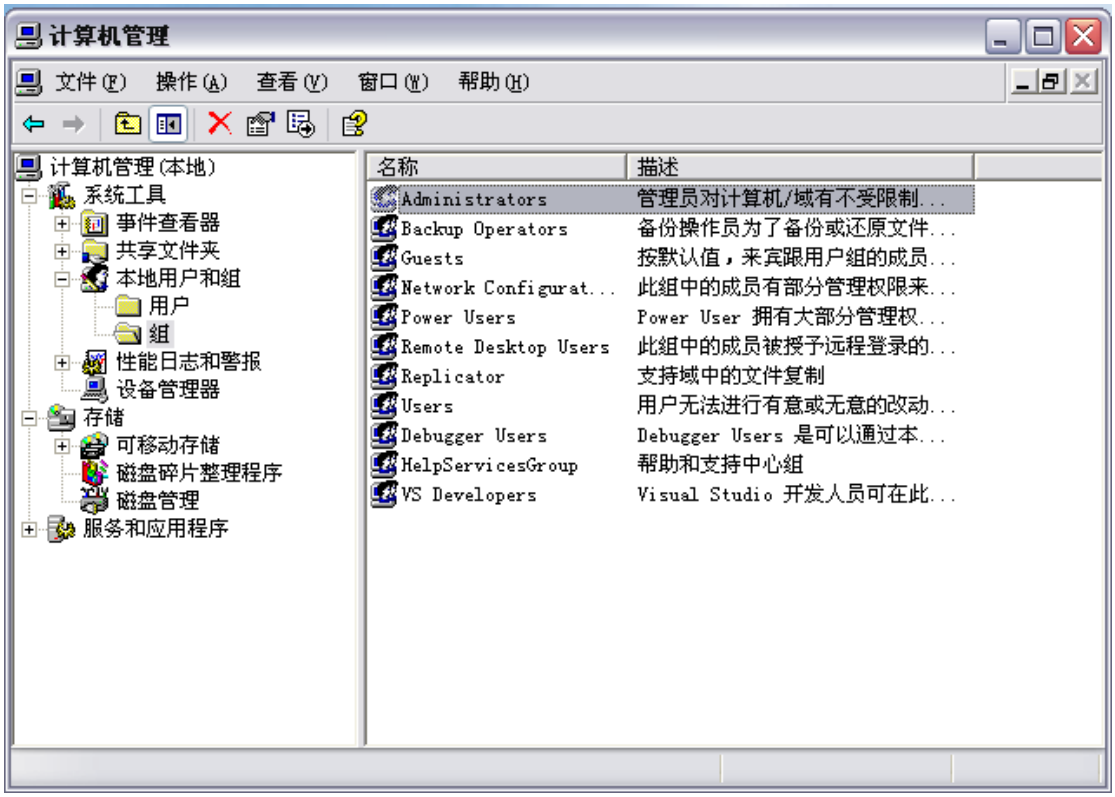
（2）加入过域，登录域正常但用 MRAM 发现时无法发现

原因：被监控本身保存在本机上的域信息中只保留了登录过本机账号的信息，机器上域的一些相关信息由于长时间使用已经失去时效性，只能验证本地或登录过本地的域账号或本地账号，但如果被本机上不存在的用户远程登录时无法验证，需要把该用户加入到本地组中才可验证.

3) 在被监控机器上显式的添加 sc\bsmtest 的权限

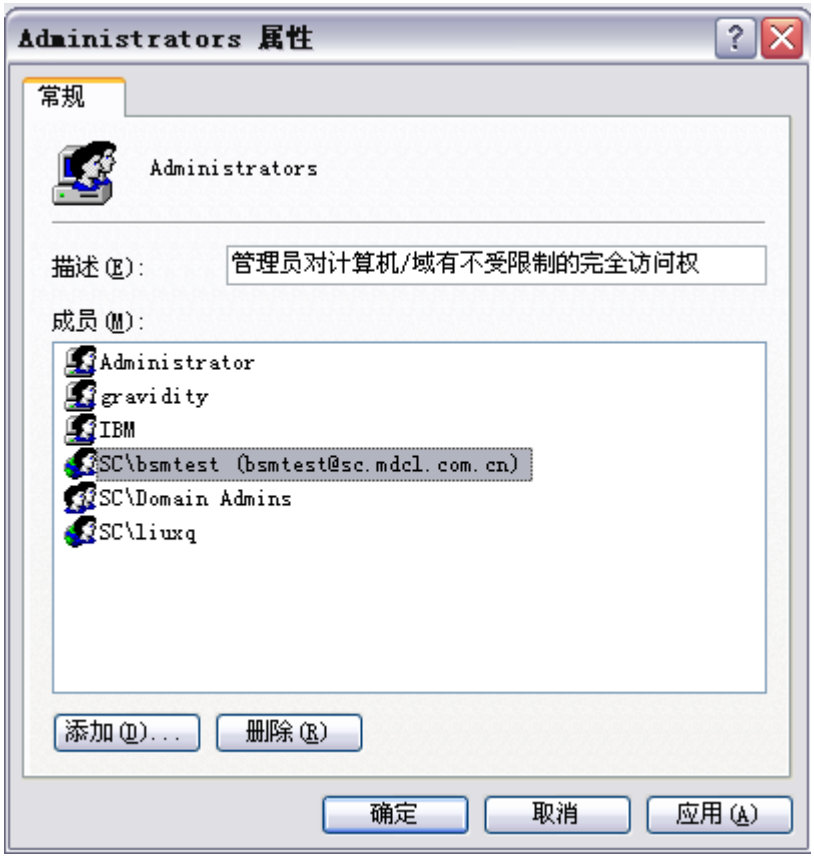
如果被监控端机器在域中，但是你不想退出域再重新加入，那么也可以用下面的办法：

1．在桌面上，右键点击“我的电脑”，选择“管理”，在弹出的对话框中，以此选择：“系统工具”，“本地用户和组”，“组”；



2．在组列表中双击“Administrators”组；在弹出的属性对话框中，选择“添加”按钮，添

加“sc\bsmtest”用户，如下图所示：

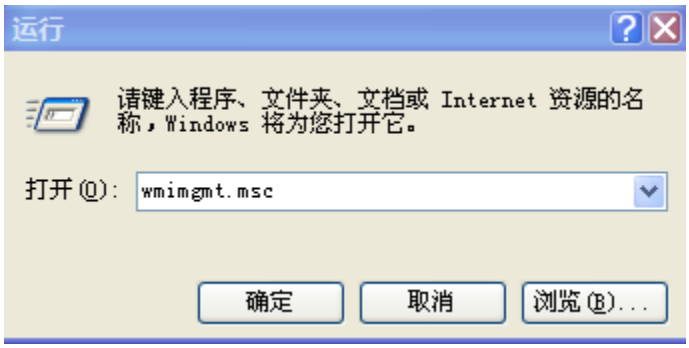


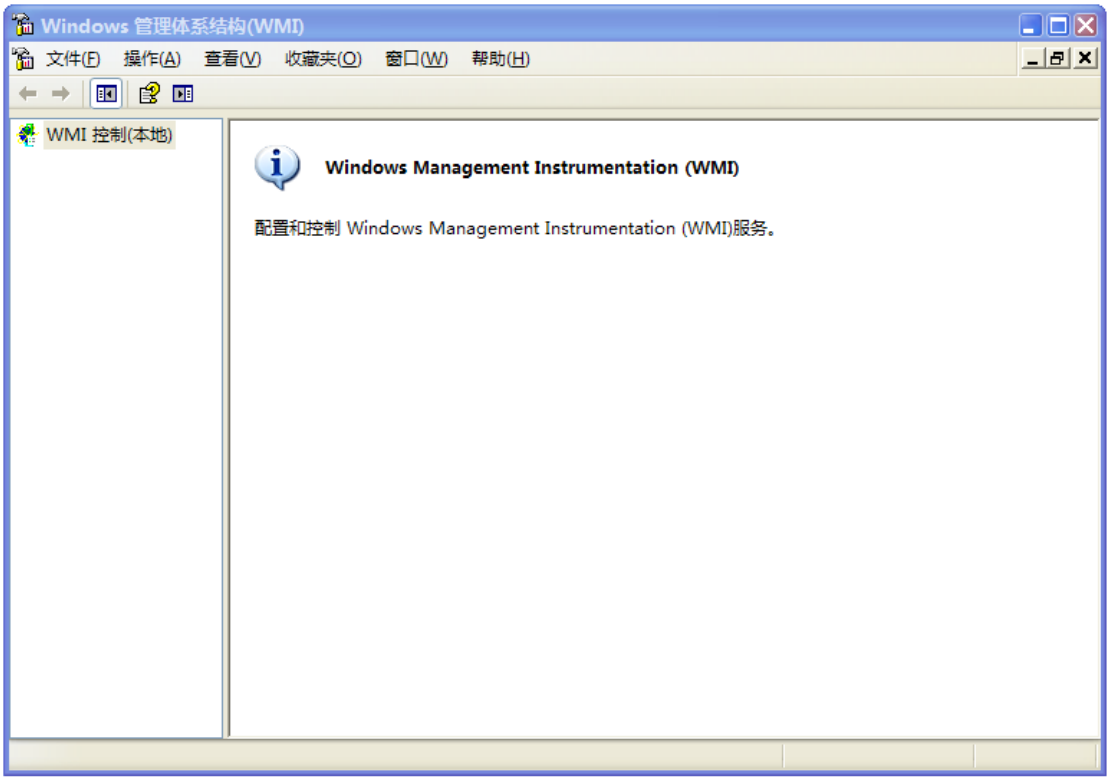
34.8. 普通账户监控

在工程现场，往往为了使 windows 普通帐户能通过 WMI 监控该 Windows 服务器，需要做如下设置，步骤如下：

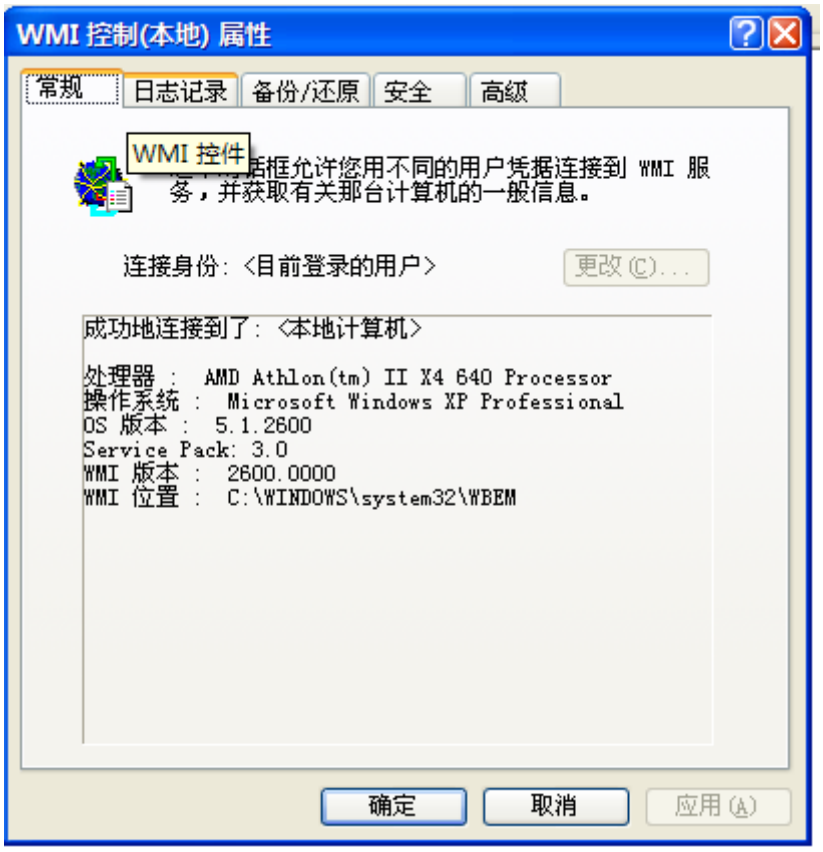
34.8.1. 命名空间访问权限设置

WIN+R

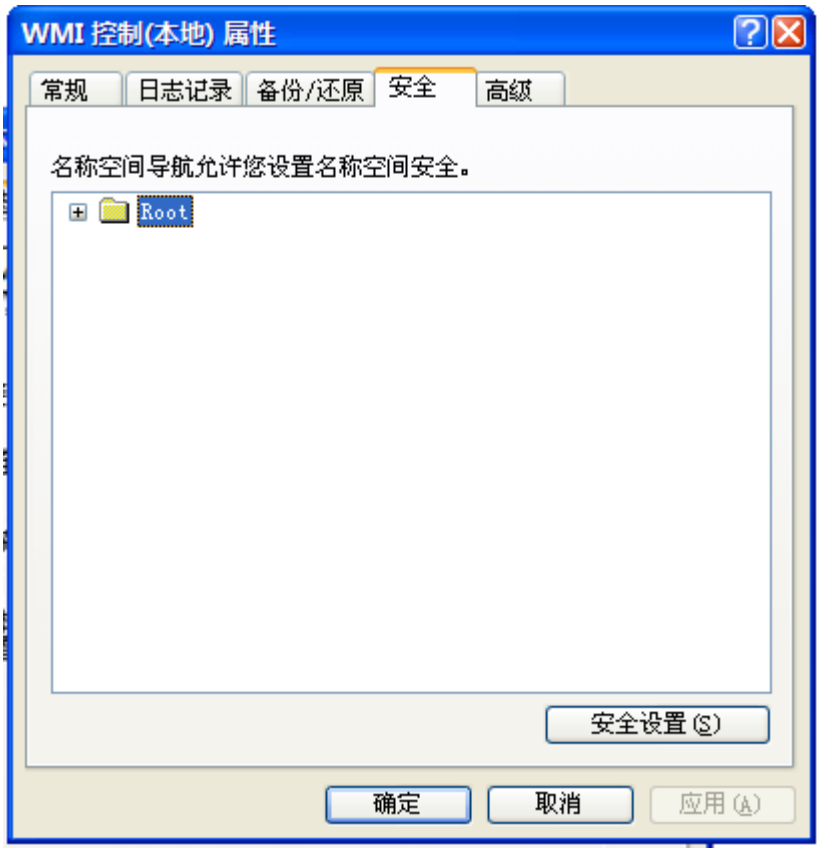




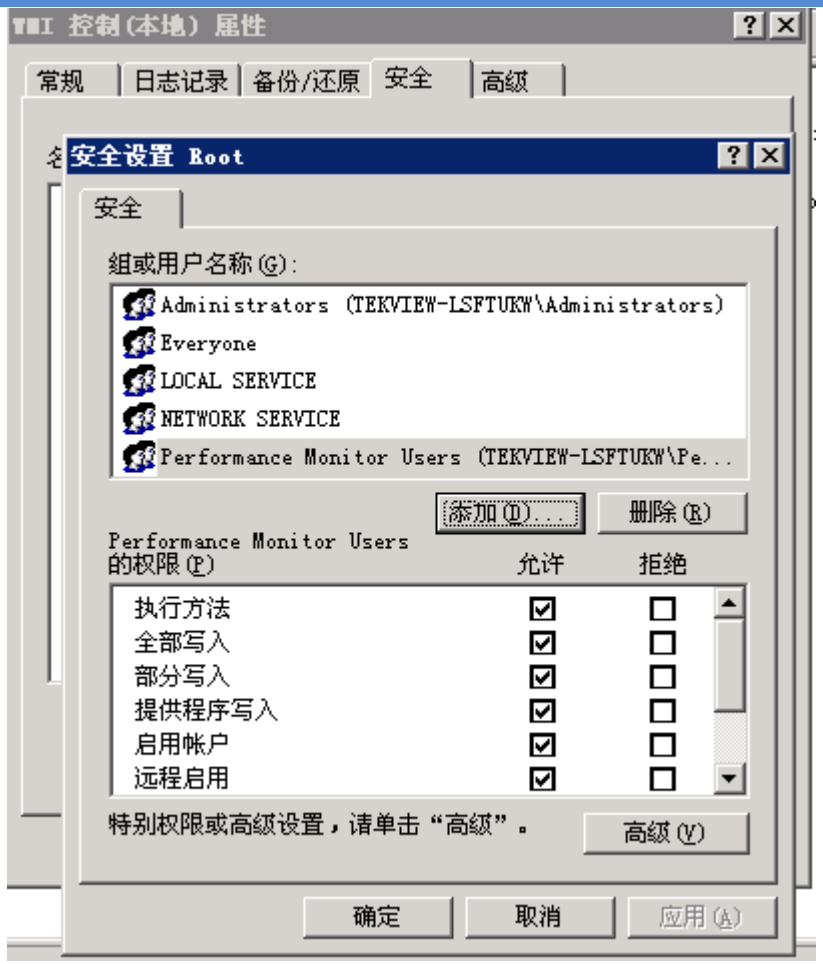
鼠标右健点击：WMI 控制(本地)—>属性



选择“安全”


WMI 控制(本地) 属性
常规
日志记录
备份/还原
安全
高级
名称空间导航允许您设置名称空间安全。
Root
安全设置(S)
确定
取消
应用(A)

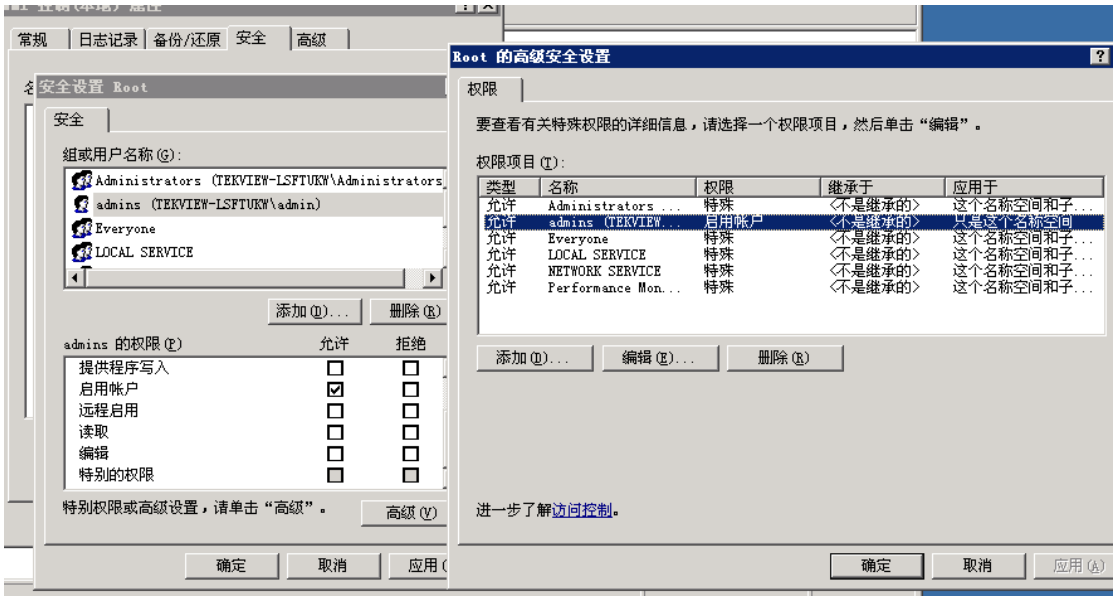
单击“安全设置”



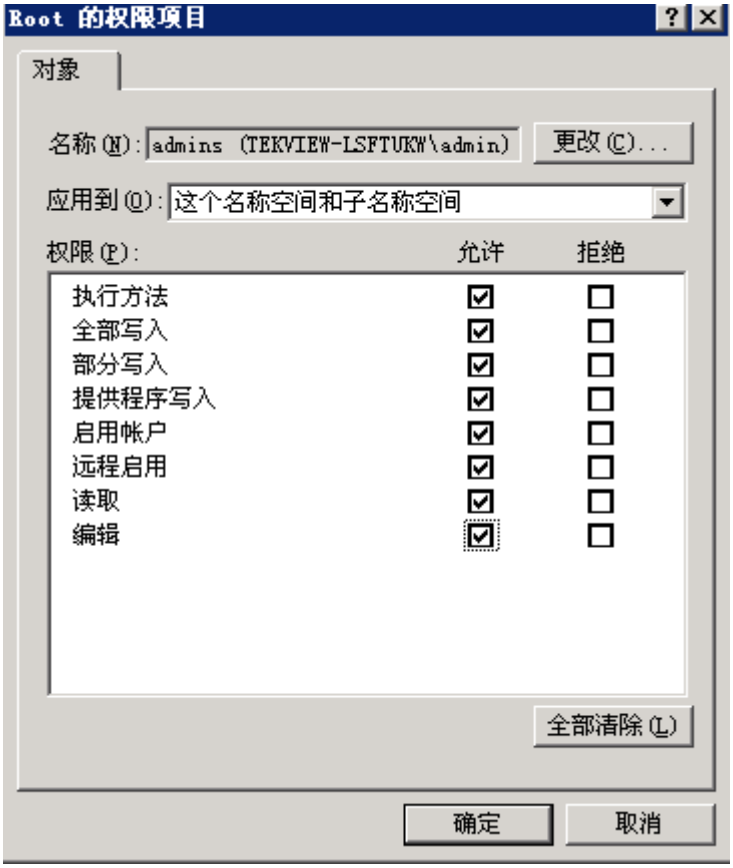
如果用户或用户所在的组不在列表中，单击“添加”

输入用户名或用户组名，点击“检查名称”，确认无误后，然后确定。

选中刚添加的用户或组，点“高级”，弹出窗口如下：



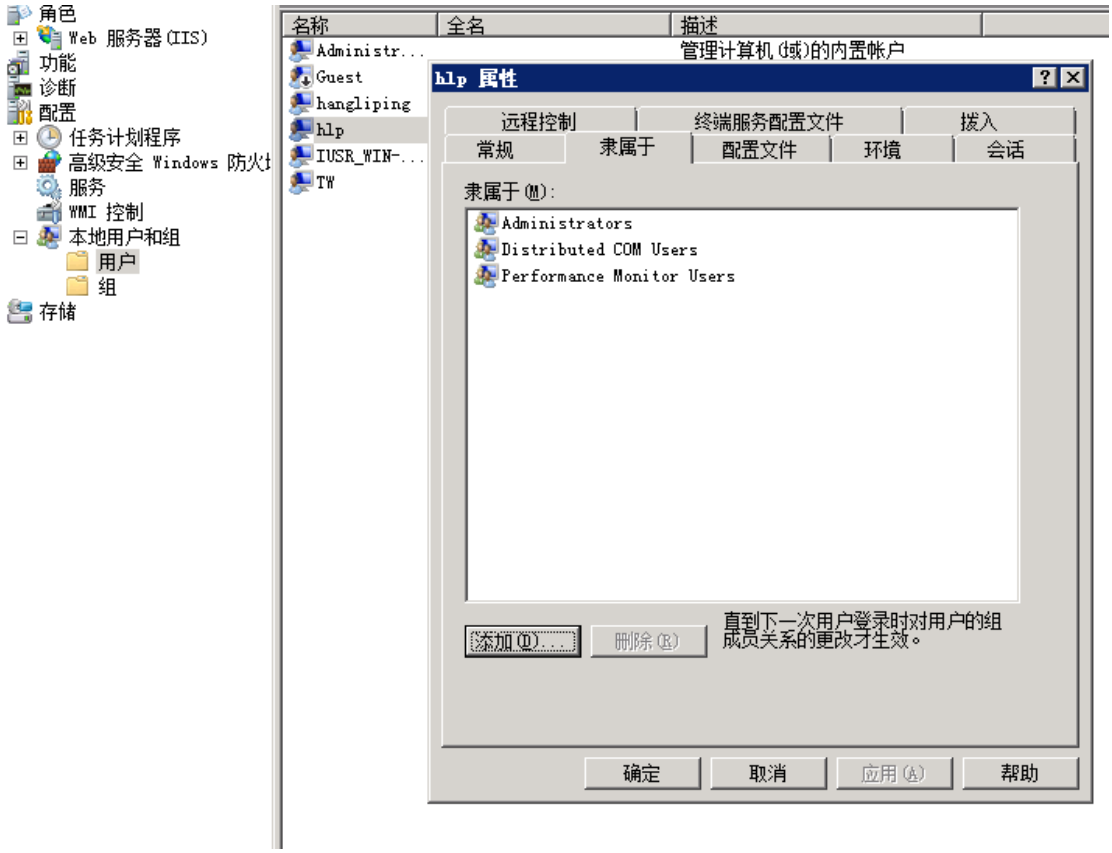
双击添加的用户名或组名为其分配权限，如下图



应用到：选中“这个名称和子名称空间”
权限：允许 checkbox 全部选择

点击确定

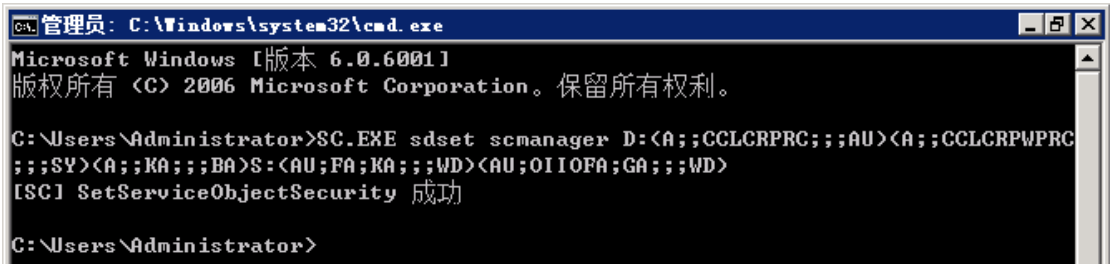
注意：监控帐号必须隶属于 Distributed COM Users 和 Performance Monitor Users 用户组，否则可能会造成部分数据比如服务器 CPU 使用率、磁盘 IO 信息读取失败，如果出现这种情况，请将该账户加入到这 2 个组中，参见下图：



34.8.2. 系统服务对象访问权限设置

当使用非超级管理员账号通过 WMI 技术对远程服务器监控时，有时会发现无法读取远程服务器上的系统服务列表，导致无法选择远程服务器上的某些重要的系统服务进行监控，这是因为 Windows 服务器操作系统默认情况下限制了普通账号通过 WMI 远程读取的权限，此时可通过如下方式解决：

使用超级管理员帐号到远程计算机上执行命令 SC.EXE sdset scmanager D:(A;;CCLCRPRC;;;AU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)



执行成功后 Windows 普通账户就能获取远程计算机上的服务列表。

34.9. 其它设置

1. 验证用户权限

在远程计算机点击开始 --> 运行 --> 输入 gpedit.msc. 打开组策略控制台。
点击本地计算机策略 -- > 计算机配置 -- > Windows 设置 -- > 安全设置 -- > 本地策略 -- > 用户权利指派 -- > 身份验证后模拟客户端。
添加用户后，再尝试添加服务器。以 WMI 模式添加 Windows 监视器，要求用户具有管理员权限。

2. 本地安全设置

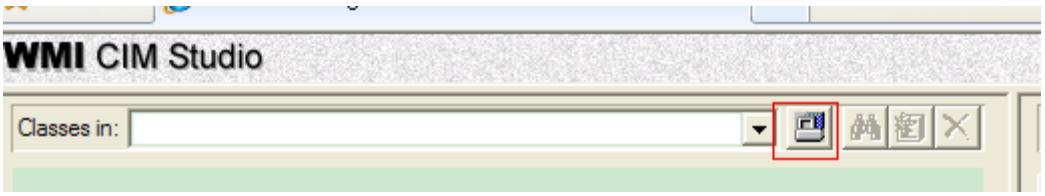
如果远程机器是 Windows XP 计算机， 确保远程登录不强制使用 GUEST 帐户。点击开始 --> 运行 --> 输入 secpol.msc，打开本地安全设置控制台。点击本地策略 ->安全选项 -> 网络访问：本地帐户的共享和安全模式，如果设置为仅来宾，则右键点击属性，更改为经典，然后重启计算机。

34.10. 测试 WMI 远程监控

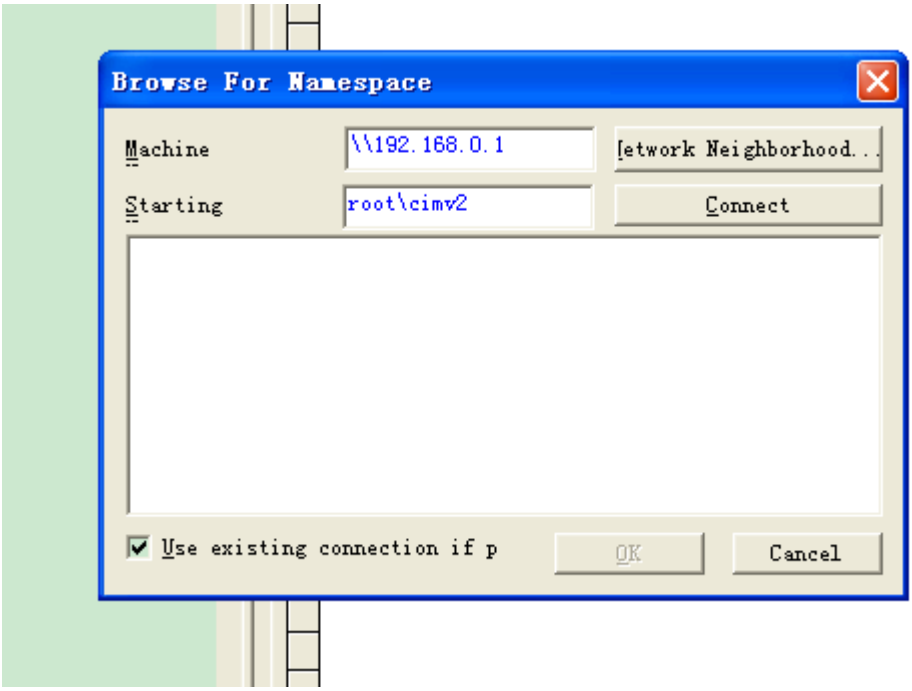
为了测试远程计算机可以通过 WMI 进行监控和管理，在远程计算机上做了相应配置后，可以使用微软提供的 WMITools 工具在本地连接到远程计算机进行测试。

测试工具：WMITools.exe
下载地址：http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=24045

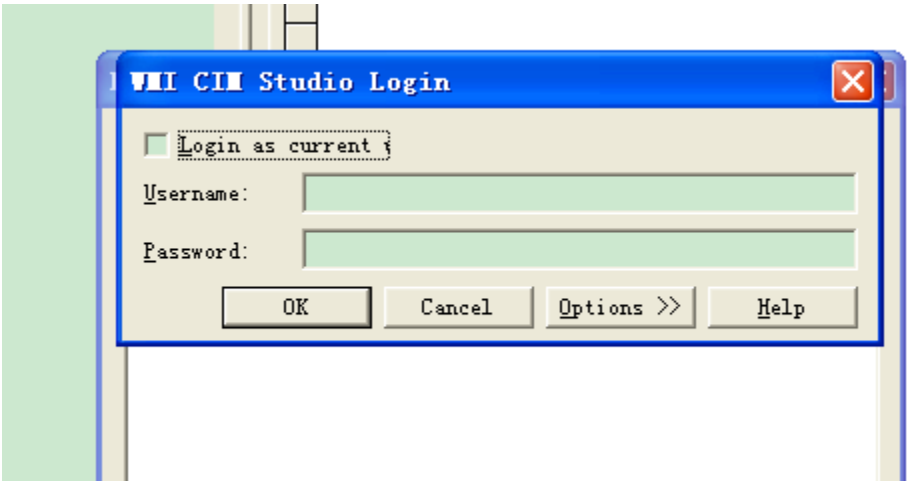
安装完成后点击：wmi-studio
点击



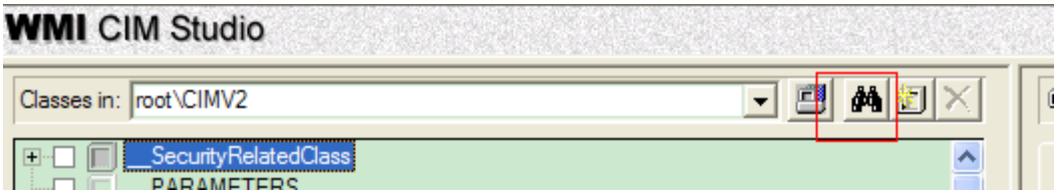
填写机器 IP，开始的命名空间



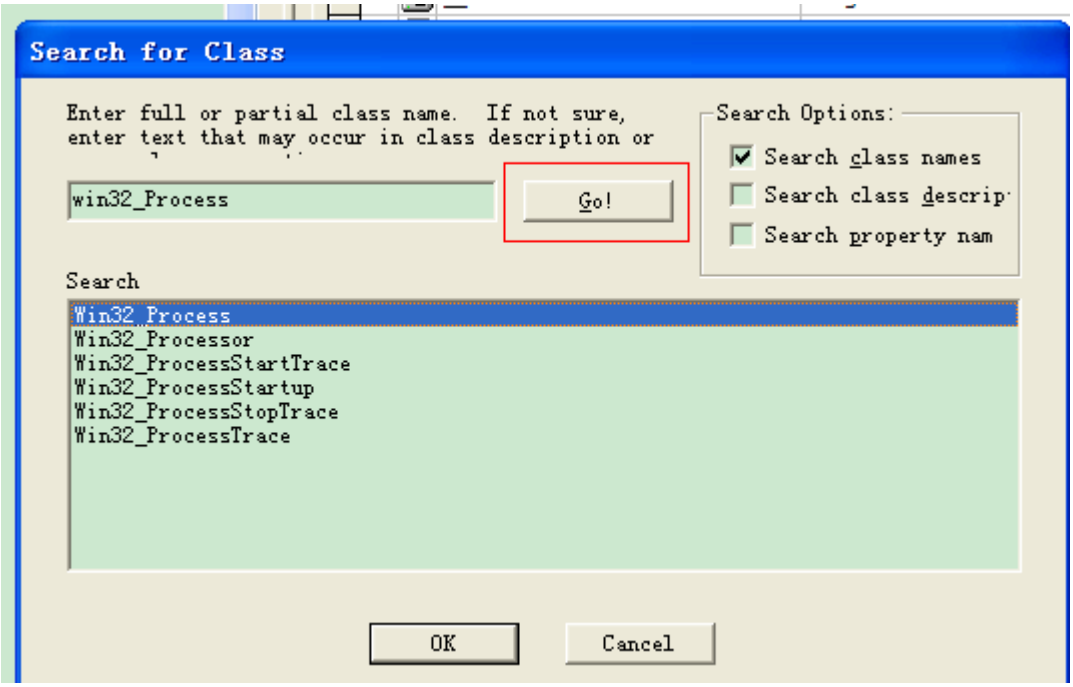
然后点击 Connect，填写用户名，密码（注意本机不需要用户名密码）



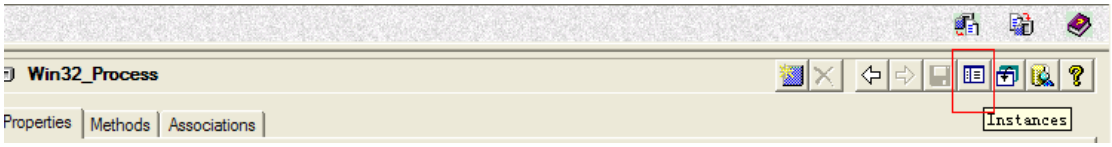
连接成功后，如果需要查询 wmi 类点击



例如查询 windows 进程类 win32_Process



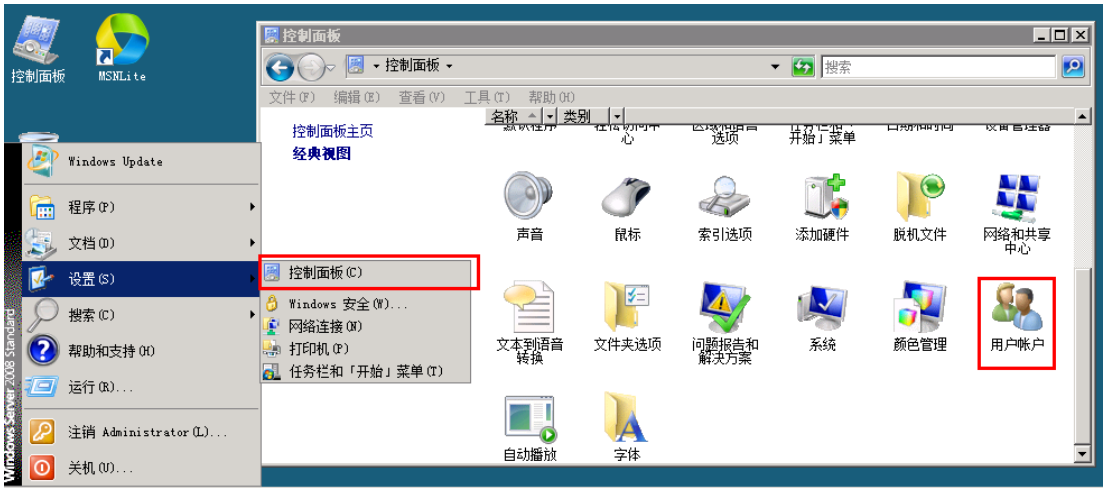
点击 Instances 便可查看进程相关数据



34.11. Windows Server 2008/2008 R2/2003 UAC 关闭方法

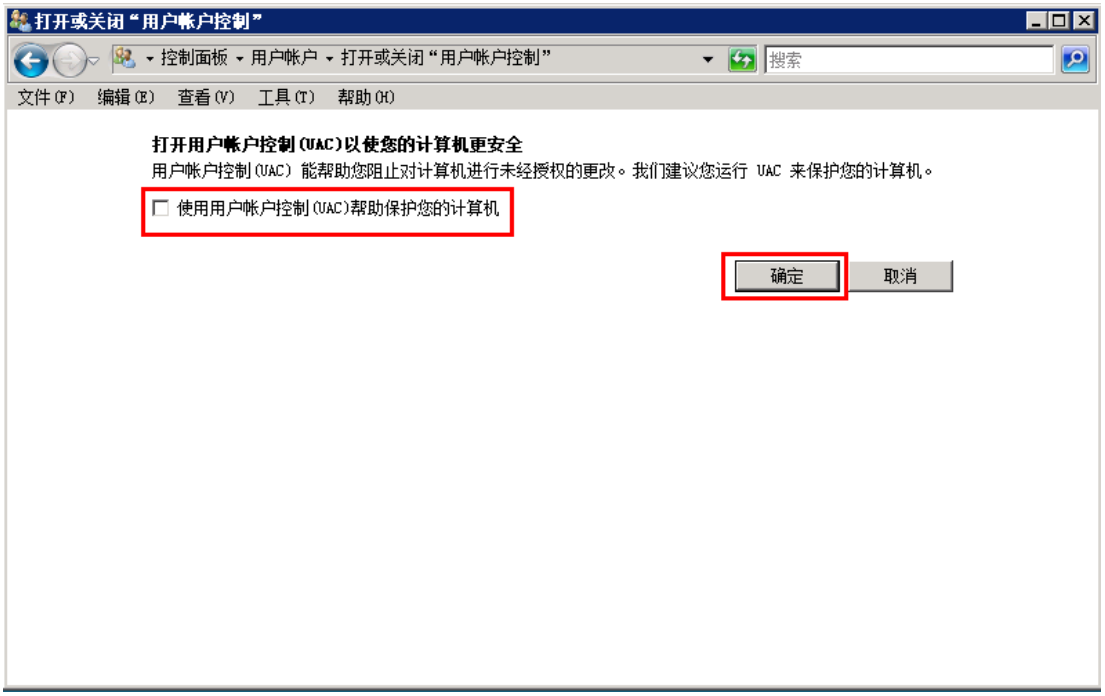
方法一

1、点击菜单“开始->控制面板”，进入系统的控制面板，选择“用户帐户”，如下图所示：



2、点击“打开或关闭“用户帐户控制””

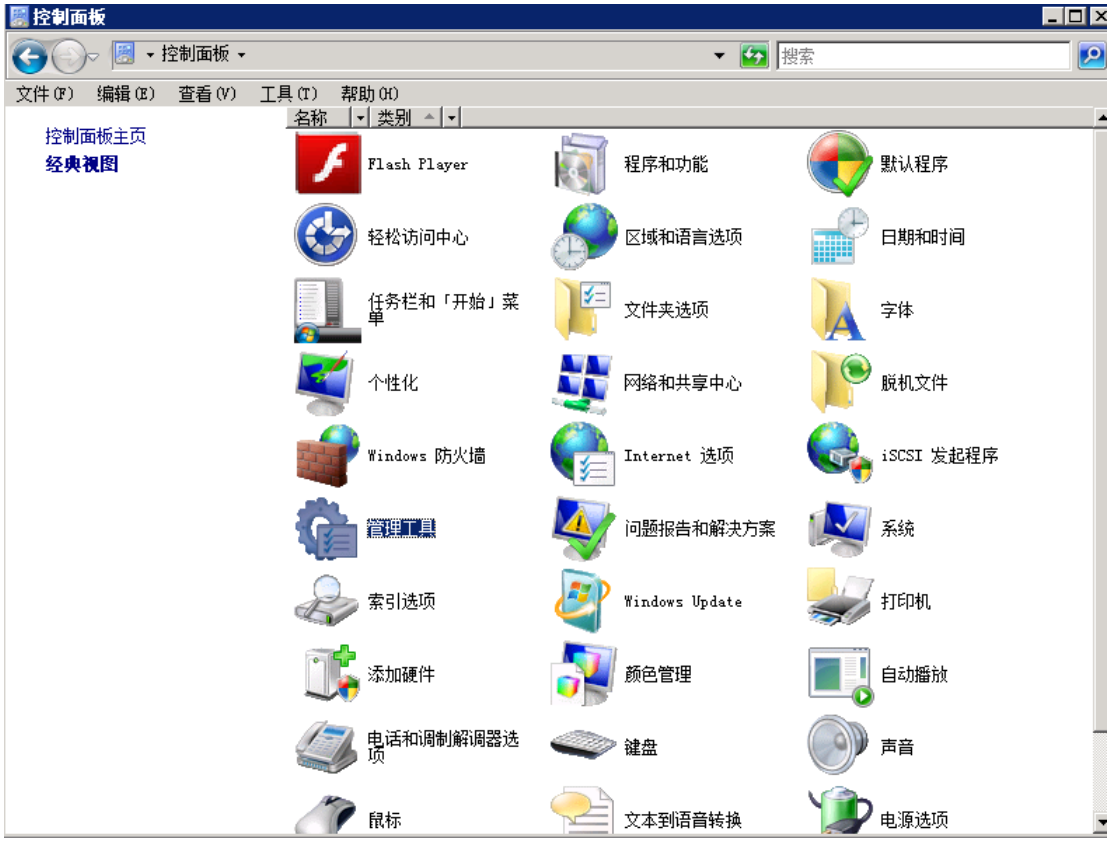
3、进入下图界面，取消选中的复选框，然后点击“确定”按钮即可



4、重启服务器。

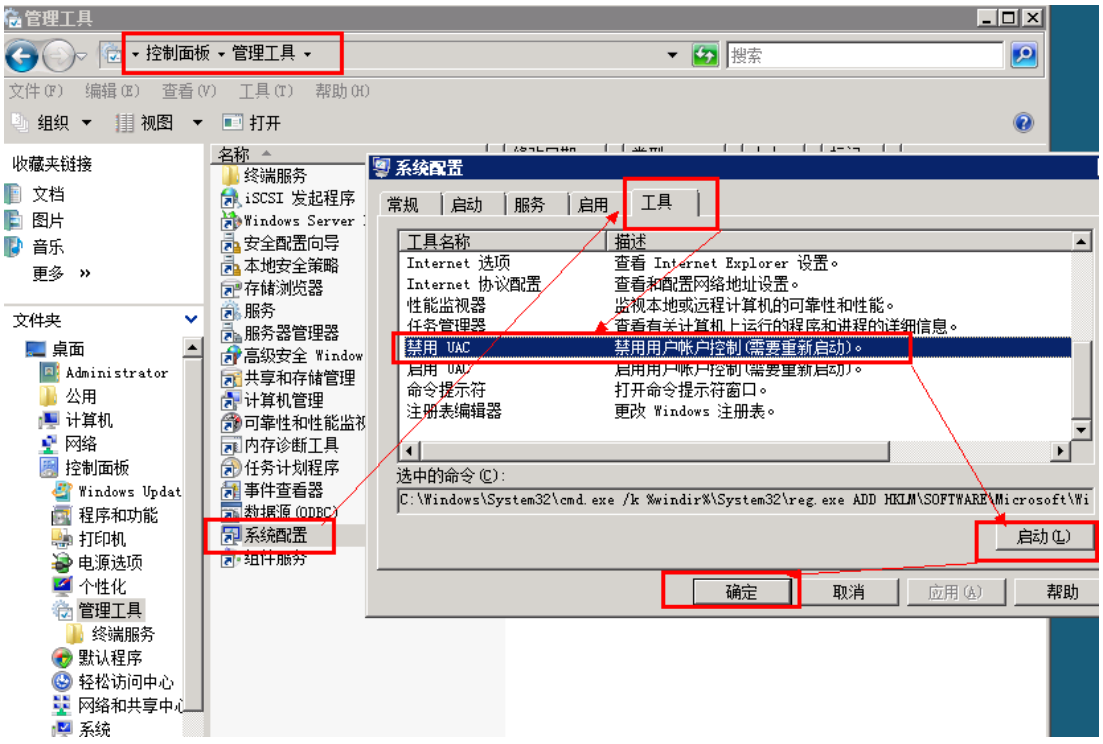
方法二

1、点击菜单“开始->控制面板”，进入系统的控制面板，双击“管理工具”，如下图所示：



2、双击

“系统配置”，在弹出的对话框中选择“工具”，找到“禁用 UAC”选项，然后点击“启动”按钮，再次点击“确定”按钮，如下图所示：



3、重启服务器。

注：Windows Server 2008R2 有所不同，仍然在控制面板→用户帐户→用户帐户→改变 UAC 设置→选择永不通知，2008R2 则并**不需要重启服务器**。

Windows2003 没有关闭 UAC 选项，而且我们也不建议关闭 UAC，如果用户想强制关闭，可参考如下脚本：
C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
拷贝到文本文件，修改类型为.bat。

35. DNS 服务监控

1. 确定 DNS 服务的 IP 地址
2. 给定用来做 DNS 解析测试的域名，该域名要存在于 DNS 服务器中
3. 给定 DNS 解析的超时时间和记录类型（一般选择 A 记录即可，表示 Address）

36. LDAP 服务监控

1. 确保 LDAP 服务正在运行，从管理员处获取连接到 LDAP 服务的 IP 地址、用户名、密码及端口（端口号默认是 389）。
2. 从管理员处获取 LDAP 服务的查询 Base，这是一个字符串，添加 LDAP 服务资源时需要输入该字符串。
3. 从管理员处获取 LDAP 服务的查询过滤器，这是一个字符串，添加 LDAP 服务资源时可以使用该字符串来限定查询范围（可选）。

37. Exchange 邮件服务器

通过 WMI 协议监控 Microsoft Exchange Mail Server，支持 Exchange 2010。

当 Windows 服务器上安装了 Exchange 邮件系统时，安装程序会自动注册和 Exchange 邮件服务相关的 WMI 对象，此时客户端管理软件可以通过 WMI 协议查询到 Exchange 邮件服务的相关状态、性能信息。

当需要监控 Exchange 邮件服务器时，必须确保远程 Windows 服务器 WMI 相关的设置正确，如果 WMI 配置不正确，则无法对 Exchange 邮件服务器进行监控，如何配置 Windows 操作

系统的 WMI 协议，请参考 Windows 服务器监控章节。

38. IBM DS 系列磁盘阵列

支持监控 IBM DS 系列中的中低端产品（http://www-03.ibm.com/systems/cn/storage/disk/?re=masthead），包括 IBM DS3200、IBM DS3300、IBM DS3400、IBM DS3500、IBM DS4000、IBM DS4100、IBM DS4200、IBM DS4300、IBM DS4400、IBM DS4500、IBM DS4700、IBM DS4800、IBM DS5000。

对 DS 系列中的中低端产品的监控，通过 IBM 配套的存储管理软件（DS Storage Manager）进行，请按照下述步骤进行：

1. 将 Probe 与 DS Storage Manager 软件安装在同一台服务器上，并将 Storage Manager 软件命令行工具添加到系统环境变量中，Probe 将通过调用 DS Storage Manager 软件提供的命令行工具对获取目标存储设备的基本信息和性能统计数据。

2. 在 IM 系统中添加存储设备的实例，输入存储设备的 IP 地址、轮询周期即可进行监控。

3. 使用到的 Storage Manager 命令及参数如下所示：

    1. 获取基本数据，尝试下列 2 条命令，替换其中的 ipAddress

        SMcli ipAddress -c "show storagesubsystem profile;"
        SMcli ipAddress -c "show storagearray profile;

    2. 获取性能数据：根据 ip 地址获取，尝试下列 4 条命令，替换其中的 ipAddress

SMcli ipAddress -c "set session performanceMonitorInterval=PERF_ITVL performanceMonitorIterations=1; show allLogicalDrives performanceStats;"

SMcli ipAddress -c "set session performanceMonitorInterval=PERF_ITVL performanceMonitorIterations=1; show allVolumes performanceStats;"

SMcli ipAddress -c "set session performanceMonitorInterval=PERF_ITVL performanceMonitorIterations=1; show storageSubsystem performanceStats;"

SMcli ipAddress -c "set session performanceMonitorInterval=PERF_ITVL performanceMonitorIterations=1; show storageArray performanceStats;"

根据系统名称获取，尝试下列 4 条命令，替换其中的 systemName
SMcli -n systemName -c "set session performanceMonitorInterval=PERF_ITVL performanceMonitorIterations=1; show allLogicalDrives performanceStats;"

SMcli -n systemName -c "set session performanceMonitorInterval=PERF_ITVL performanceMonitorIterations=1; show allVolumes performanceStats;"

SMcli -n systemName -c "set session performanceMonitorInterval=PERF_ITVL performanceMonitorIterations=1; show storageSubsystem performanceStats;"

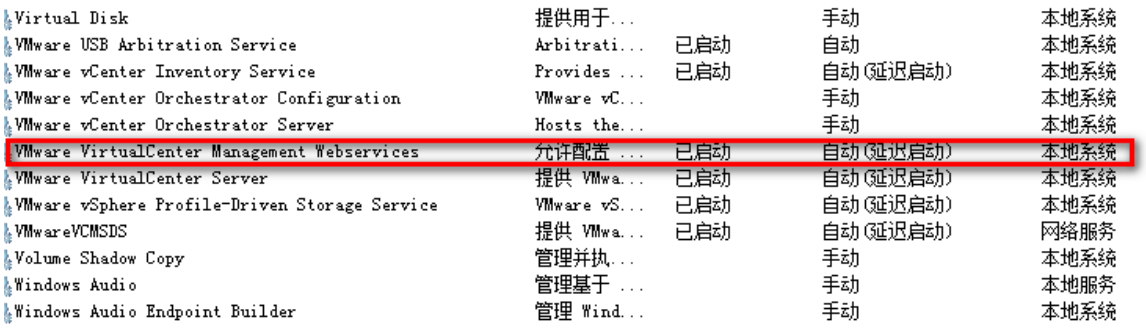
SMcli -n systemName -c "set session performanceMonitorInterval=PERF_ITVL performanceMonitorIterations=1; show storageArray performanceStats;"

39. vmware

39.1. 与 vmware vSphere5.0、5.1 版本的集成

支持与 vmware vSphere5.0、5.1 版本的集成，请按照如下步骤进行：

1. 确认 vCenter Server 的 webservice 服务正在运行，如下图所示：



2. 与 vCenter server 的集成是通过基于 HTTPS 协议的 WEB SERVICE 进行，请确认采集器能够访问 vCenter Server 的 TCP 443 端口，该端口是 HTTPS 协议的默认监听端口

3. 使用浏览器打开 APEX IT 综合监控系统客户端，选择【虚拟化管理】-【VMware】，点击添加按钮，输入 vCenter Server 服务的名称、IP 地址、端口、用户名、密码、状态轮询周期、同步周期，选择相应的 Probe 采集器，点击“确定”按钮，如果参数正确的话，将能够保存成功，如果添加失败，请仔细检查各项参数，以及服务器的防火墙配置。

4. 如果有多台 vCenter Server 需要添加，请重复步骤 1，2，3。

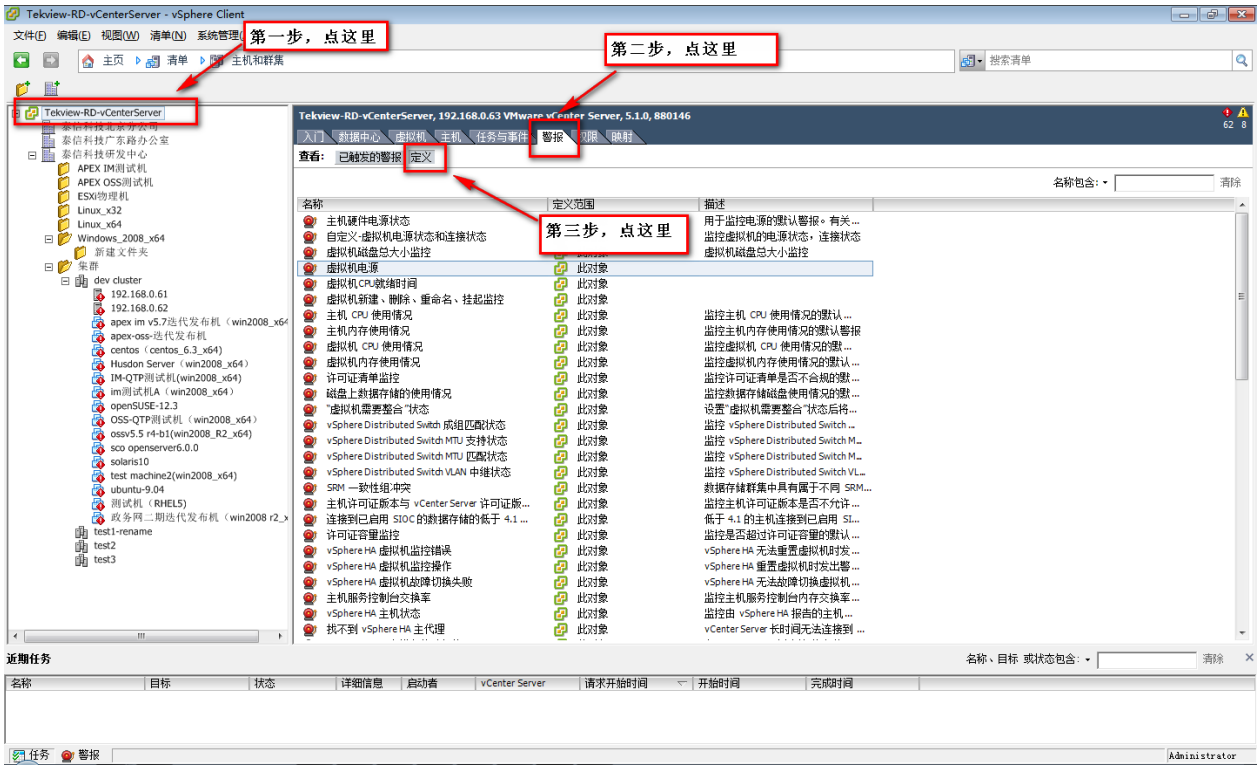
5. 添加 vCenter Server 成功后，等待片刻，采集器会自动从 vCenter Server 中通过 WEB SERVICE 协议获取各种数据，包括虚拟化环境中的数据中心、ESX/ESXi 主机、已经创建的各种虚拟机、Datastore、集群，并获取这些组件的实时性能数据和状态数据。

6. 配置 vCenter Server 的 SNMP Trap，以便当故障发生后，vCenter Server 能够将告警通过 SNMP Trap 的方式发送给 APEX Trap 接收器，请按如下步骤进行：

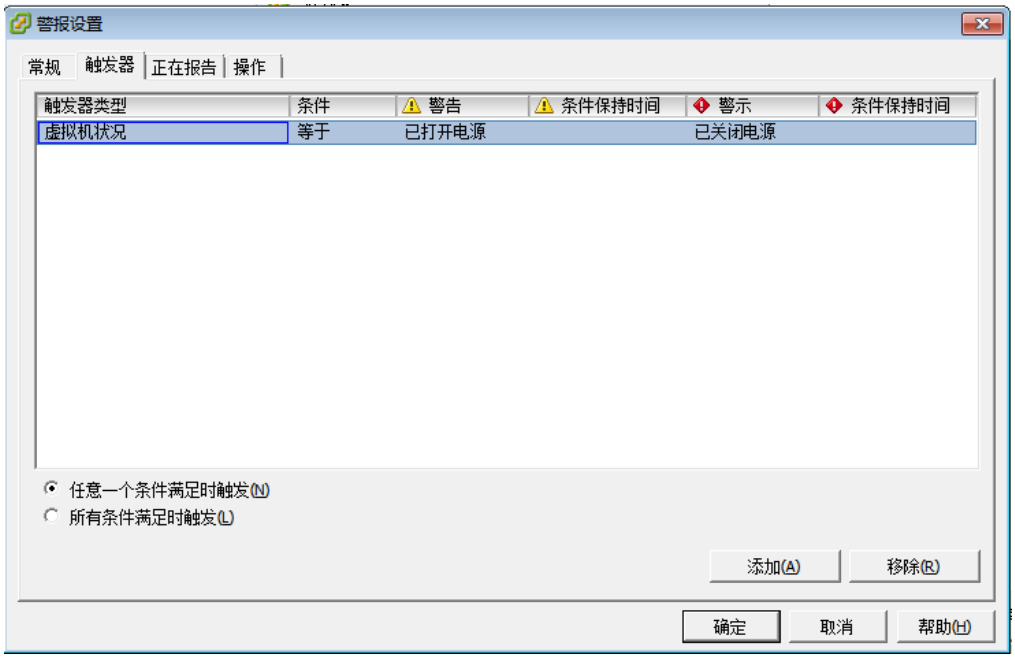
1. 打开 vSphere client 并登录，登录成功后选择【系统管理】-【vCenter Server 设置】，从左边的导航菜单中选择【SNMP】，在右边的 SNMP 收件人中输入接收 SNMP Trap 的主机 IP 地址、端口和读共同体。

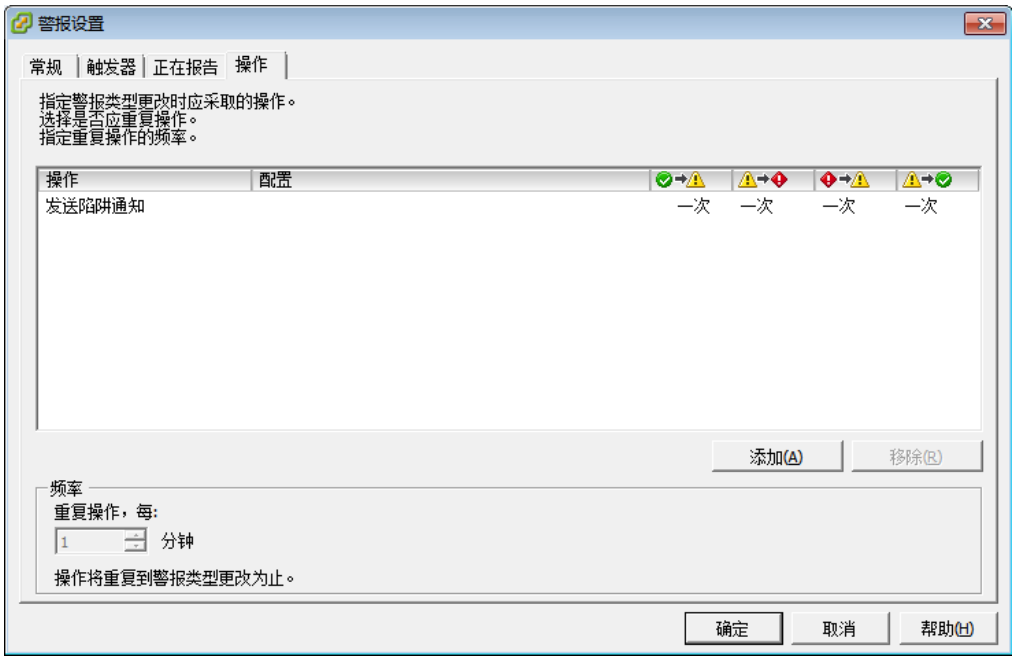
2. 修改现有 vCenter Server 中的警报配置项（或者新建警报配置），在“警报设置”对话框中，将“操作”选项中的操作类型修改为“发送陷阱通知”，并配置陷阱发送的次数，比如正常状态到黄色级别告警、黄色级别告警到红色级别告警、黄色级别告警恢复到正常状态时，vCenter Server 发送的 SNMP Trap 陷阱的次数，可以选择一次或重复发送。

注意：在配置警报的时候，要针对全局进行设置，意思就是创建的警告策略是覆盖整个 vCenter Server 的，而不是针对某个数据中心或 ESXi/ESX 主机进行的，这样可以减少配置的警报数量，如果不是针对全局进行的设置，就有可能导致某些主机的告警可以发送，某些主机的告警不能发送。当然，实际情况下如果需要分开设置的话也可以分开设置，比如按照数据中心来设置警报策略。



注意：如何配置 vCenter Server 的警报，请参考 vmware vSphere 服务器虚拟化软件的用户手册，这里不做详细描述，我们假设您已经理解相关理论知识且熟悉 vmware 公司的 vSphere Client 软件的各种操作。





3. 确保 APEX IT 综合监控系统的 nms-tss 组件正常启动，该组件用来接收任意第三方系统发送的 SNMP Trap 消息，并将 SNMP Trap 消息转化为 APEX 告警模块的标准告警格式，对 vCenter Server 发送出来的 SNMP Trap 消息，也需要该组件正常运行。

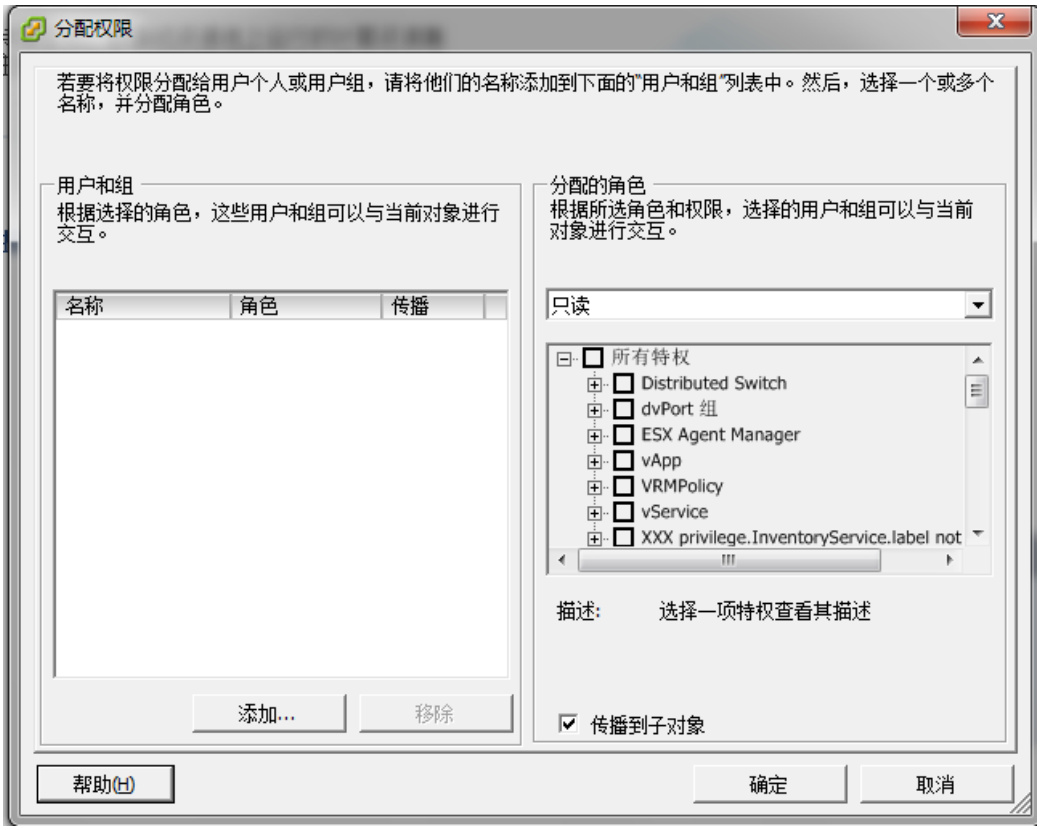
4. 如果需要接收到 vCenter Server 的 SNMP Trap 消息后执行告警动作，请以管理员身份登录 APEX IT 综合管理系统，点击【系统管理】-【全局参数设置】-【系统告警设置】，在右边的界面中配置各个级别的 Trap 告警关联的告警动作后点击页面最下方的确定按钮。

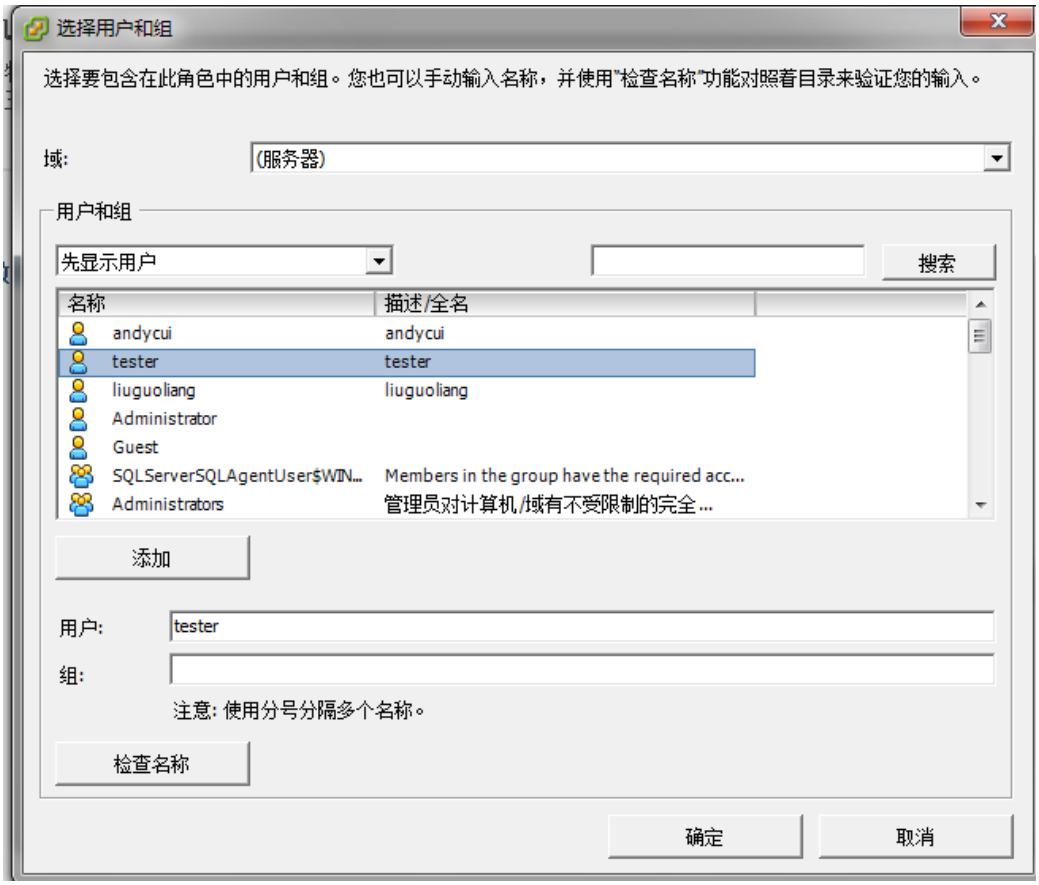
39.2. 为监控 VMWare 创建专用帐号

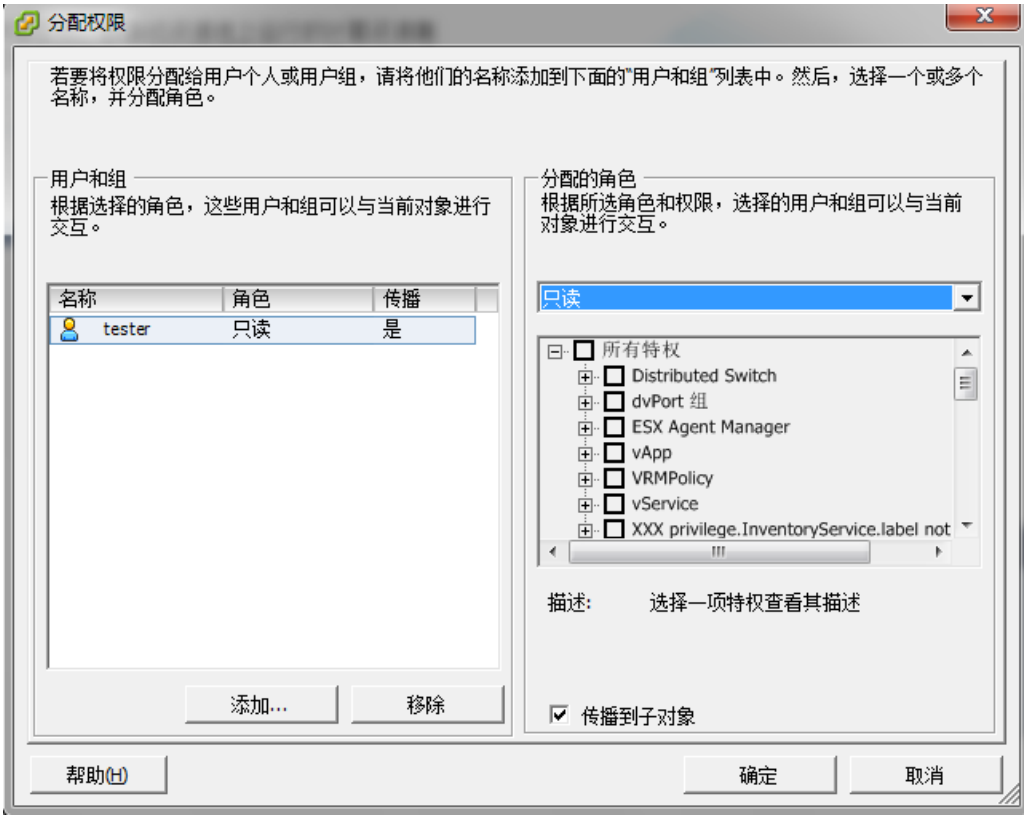
为了安全起见，在监控 VMWare 时，可专门为其创建一个只读帐号，步骤如下:

1. 登陆到 VMWARE 服务器，创建一个系统 guest 帐号，如 tester
2. 通过 vShpere Client，以 Administrator 身份登陆到 vCenterServer，选中数据中心根节点，右键选中添加权限菜单，如下图

3. 当点击添加权限菜单后，弹出分配权限窗口，在弹出的窗口中选择添加。会列出之前创建好的帐号，如 tester，选中 tester，确定，再为该用户分配只读角色。


分配权限
若要将权限分配给用户个人或用户组，请将他们的名称添加到下面的"用户和组"列表中。然后，选择一个或多个名称，并分配角色。
用户和组
根据选择的角色，这些用户和组可以与当前对象进行交互。
名称
角色
传播
添加...
移除
分配的角色
根据所选角色和权限，选择的用户和组可以与当前对象进行交互。
只读
所有特权
Distributed Switch
dvPort 组
ESX Agent Manager
vApp
VRMPolicy
vService
XXX privilege.InventoryService.label not
描述:
选择一项特权查看其描述
传播到子对象
帮助(H)
确定
取消


选择用户和组
选择要包含在此角色中的用户和组。您也可以手动输入名称，并使用"检查名称"功能对照着目录来验证您的输入。
域:
(服务器)
用户和组
先显示用户
搜索
名称
描述/全名
andycui
andycui
tester
tester
liuguoliang
liuguoliang
Administrator
Guest
SQLServerSQLAgentUser$WIN...
Members in the group have the required acc...
Administrators
管理员对计算机/域有不受限制的完全...
添加
用户:
tester
组:
注意: 使用分号分隔多个名称。
检查名称
确定
取消



4. 创建成功后，在添加监控 VMWARE 的页面就可以用此帐号。

40. HDS (SMI-S)

HDS 的 SMI-S Provider 由 HDS DeviceManager 软件提供，实现通过 SMI-S 协议对 HDS 磁盘阵列进行监控，安装任意平台的 HDS DeviceManager 软件，为了部署方便，建议安装 windows 版本。

1. 将要管理的 HDS 磁盘阵列添加到 DeviceManager 中，如果有多台，请依次添加

2. 在 APEX 系统中添加 HDS 磁盘阵列时，输入 DeviceManager 的 IP 地址、端口、用户名、密码、名称空间，点击测试按钮，系统会自动发现 DeviceManager 中管理的所有磁盘阵列，选择需要进行监控的磁盘阵列后，点击确定即可

3. 注意：名称空间，如果 DeviceManager 软件的版本是 v5.8 或 v5.8 之前的版本，则名称空间是：/root/hitachi/smis<xx>，xx 是 SMI-S 的版本号；如果是 v5.8 之后的版本，则名称空间是：/root/smis/current

41.EMC CX 系列

通过 Navisphere CLI 工具软件实现对 EMC CLARiiON 系统磁盘阵列的监控。

1. 安装 windows 版本的 Navisphere CLI 客户端工具软件，下载地址：http://180.169.30.194/?p=861 下载

2. 将 NaviCLI.exe 所在的文件夹目录添加到系统环境变量中

3. 在确保 EMC 存储服务器在开启了 NaviCLI 服务的情况下，可通过下面命令去进行测试并将测试结果重定向到文本文件。

无密码：

```
D:\Program Files\EMC\Navisphere CLI 6.26.32.0.72>navicli -h ipAddrss getall > d:\result.txt
```

有密码：

```
D:\Program Files\EMC\Navisphere CLI 6.26.32.0.72>naviseccli -h ipAddress -user username -password pwd getall > d:\result.txt
```

成功执行完命令后查看一下输出 result.txt 文件中的内容是否正确。

42.EMC VNX/Symmetrix 系列

如果客户现场没有安装 EMC 公司的 SMI-S Provider 软件，按如下步骤进行：

1. 下载适用于 EMC 公司磁盘阵列的 SMI-S Provider 软件，下载地址：http://180.169.30.194/?p=869
2. 双击安装包，按照提示进行安装
3. 安装完成后，进入安装目录的 EMC\ECIM\ECOM\bin 目录，运行 TestSmiProvider，接受默认选项，然后输入 **addsys** 命令将需要监控的磁盘阵列添加到 SMI-S Provider 软件中
4. 添加成功后，进入 IM 系统，按照常规添加被监控资源的步骤进行添加即可。

注意：

1. **IM 并不直接和磁盘阵列通讯来获取数据，而是通过与 SMI-S Provider 软件进行通讯来间接获取磁盘阵列的各种数据。**
2. **SMI-S Provider 是各个磁盘阵列厂家为兼容 SMI-S 规范而各自开发的软件，可独立运行在 windows、linux 等操作系统上，不同设备厂商的软件名称各不相同，比如：**
   a) **EMC：EMC Solutions Enabler With SMI**
   b) **HP：Command View**
   c) **HDS: Device Manager**

43.NETAPP 磁盘阵列

通过 SNMP 协议对 NetApp 磁盘阵列进行监控，支持的 NetApp 磁盘阵列型号为：

NetApp FAS2040-R5

磁盘阵列上需要先启动 SNMP Agent 服务，并配置好 SNMP 读共同体。

44. IBM TS3310

对 IBM TS3310 磁带库通过 SNMP 协议进行监控，请登录设备配置 SNMP 的读写共同体。

45. IBM TS3200

对 IBM TS3200 磁带库通过 SNMP 协议进行监控，请登录设备配置 SNMP 的读写共同体。

46. Cisco FC 交换机

通过 SNMP 协议监控 Cisco FC 交换机，首先启动设备的 SNMPAgent 并配置 SNMP 读共同体，支持的 CiscoFC 交换机型号为：Cisco MDS 9100

47. IBM MQ

支持的 MQ 版本为 6.0、7.1

1. 确定要监控的 MQ 的 IP 地址和端口（默认 1414）
2. 在服务器上运行命令：dspmq，显示当前服务器上所有已经创建的队列管理器，确定需要监控的队列管理器：

3. 在服务器上运行命令：runmqsc 队列管理器的名称，进入指定的队列管理器的控制台交互窗口

4. 输入命令：display listener(*)，显示该队列管理器中配置的监听器：

```
DISPLAY LISTENER(*)
     6 : DISPLAY LISTENER(*)
AMQ8630: 显示侦听器信息详细信息。
   LISTENER(LISTENER.TCP)
AMQ8630: 显示侦听器信息详细信息。
   LISTENER(SYSTEM.DEFAULT.LISTENER.LU62)
AMQ8630: 显示侦听器信息详细信息。
   LISTENER(SYSTEM.DEFAULT.LISTENER.NETBIOS)
AMQ8630: 显示侦听器信息详细信息。
   LISTENER(SYSTEM.DEFAULT.LISTENER.SPX)
AMQ8630: 显示侦听器信息详细信息。
   LISTENER(SYSTEM.DEFAULT.LISTENER.TCP)
```

5. 找到我们关心的监听器，输入命令：display listener(监听器名称) all，按回车：

```
DISPLAY LISTENER(LISTENER.TCP) ALL
     7 : DISPLAY LISTENER(LISTENER.TCP) ALL
AMQ8630: 显示侦听器信息详细信息。
   LISTENER(LISTENER.TCP)                  CONTROL(QMGR)
   TRPTYPE(TCP)                            PORT(1415)
   IPADDR( )                               BACKLOG(0)
   DESCR( )                                ALTDATE(2013-09-29)
   ALTTIME(16.47.05)
```

根据输出的结果，我们可以看到该监听器正在 TCP 的 1415 端口监听，从而我们就可以确定 MQ 的监听端口

6. 输入命令：display chstatus(*)，获取该队列管理中配置的所有通道信息

```
DISPLAY CHSTATUS(*)
     5 : DISPLAY CHSTATUS(*)
AMQ8417: 显示通道状态细节。
   CHANNEL(QM_ORANGE.QM_APPLE)             CHLTYPE(SDR)
   CONNAME(192.168.0.27(1414))             CURRENT
   RQMNAME(QM_APPLE)                       STATUS(RUNNING)
   SUBSTATE(MQGET)                         XMITQ(QM_APPLE)
```

从上述输出中可以获取通道的名称以及接收方通道的 IP 地址和端口号，我们这里只需要获取通道的名称即可，也就是：QM_ORANGE.QM_APPLE

7. 输入命令：DISPLAY CHSTATUS(通道的名称) ALL

```
DISPLAY CHSTATUS(QM_ORANGE.QM_APPLE) ALL
     6 : DISPLAY CHSTATUS(QM_ORANGE.QM_APPLE) ALL
AMQ8417: 显示通道状态细节。
   CHANNEL(QM_ORANGE.QM_APPLE)             CHLTYPE(SDR)
   BATCHES(1)                              BATCHSZ(50)
   BUFSRCVD(5)                             BUFSSENT(6)
   BYTSRCVD(348)                           BYTSSENT(830)
   CHSTADA(2013-09-29)                     CHSTATI(17.13.22)
   COMPHDR(NONE,NONE)                      COMPMSG(NONE,NONE)
   COMPRATE(0,0)                           COMPTIME(0,0)
   CONNAME(192.168.0.27(1414))             CURLUWID(07E9475210000302)
   CURMSGS(0)                              CURRENT
   CURSEQNO(1)                             EXITTIME(0,0)
   HBINT(300)                              INDOUBT(NO)
   JOBNAME(00001DF800003408)               LOCLADDR(192.168.0.137(59944))
   LONGRTS(999999999)                      LSTLUWID(0000000000000000)
   LSTMSGDA(2013-09-29)                    LSTMSGTI(17.13.22)
   LSTSEQNO(0)                             MCASTAT(RUNNING)
   MONCHL(OFF)                             MSGS(1)
   NETTIME(0,0)                            NPMSPEED(FAST)
   RQMNAME(QM_APPLE)                       SHORTRTS(10)
   SSLCERTI( )                             SSLKEYDA( )
   SSLKEYTI( )                             SSLPEER( )
   SSLRKEYS(0)                             STATUS(RUNNING)
   STOPREQ(NO)                             SUBSTATE(MQGET)
   XBATCHSZ(0,0)                           XMITQ(QM_APPLE)
   XQTIME(0,0)                             RVERSION(07010003)
   RPRODUCT(MQMM)
```

8. 进入 APEX IT 综合管理系统【资源管理】页面，点击添加按钮，在弹出的对话框中选择 IBM MQ 后进入添加 MQ 的页面，输入要监控的 MQ 的 IP 地址、监听端口、名称、队列管理器的名称和服务器连接通道的名称，点击确定即可。

48. IBM AS400

1.安装软件

1.1 在命令行执行”GO MENU(LICPGM)”，然后选择”Option 10.Display installed licensed programs.”。

```
5722JC1     *BASE    IBM Toolbox for Java
5722TC1     *BASE    IBM TCP/IP Connectivity Utilities for i5/OS
5722XE1     *BASE    IBM eServer iSeries Access for Windows
```

要保证上面截图中的软件已安装。如果没有安装则可以通过如下步骤进行安装：

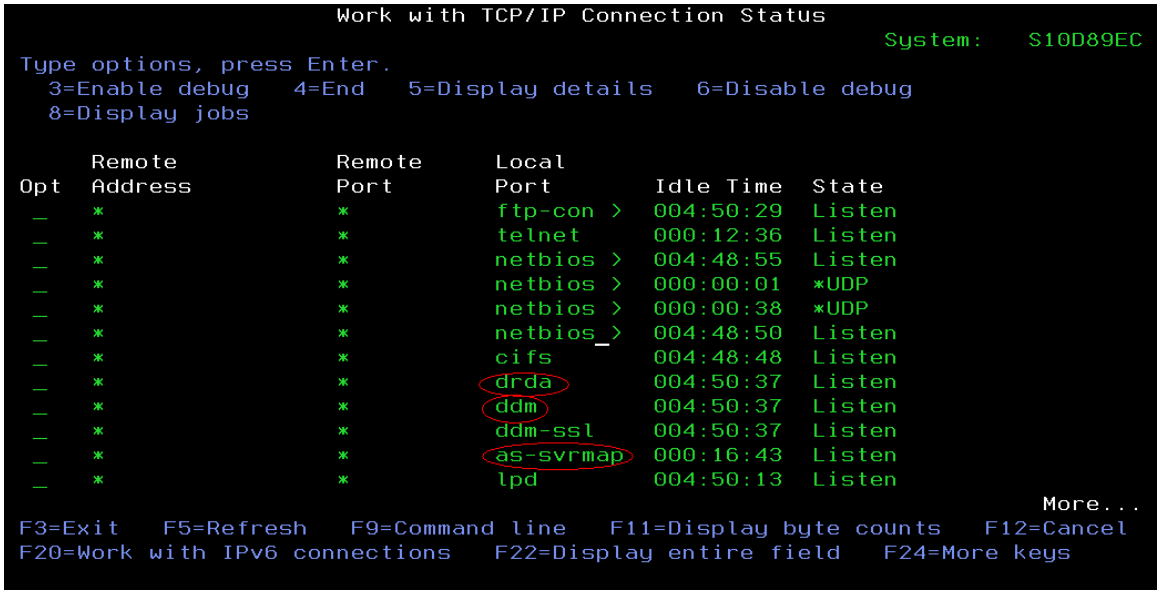
(1) 运行 CL 命令“GO MENU(LICPGM)”.

(2) 选择“Option 11. Install licensed program”选项

(3) 选择安装截图中的项。

2.启动 Host Server
在命令行处执行命令“STRHOSTSVR *ALL”

3.查看启动情况
在命令行处执行 netstat ----> 3 可进入如下界面：



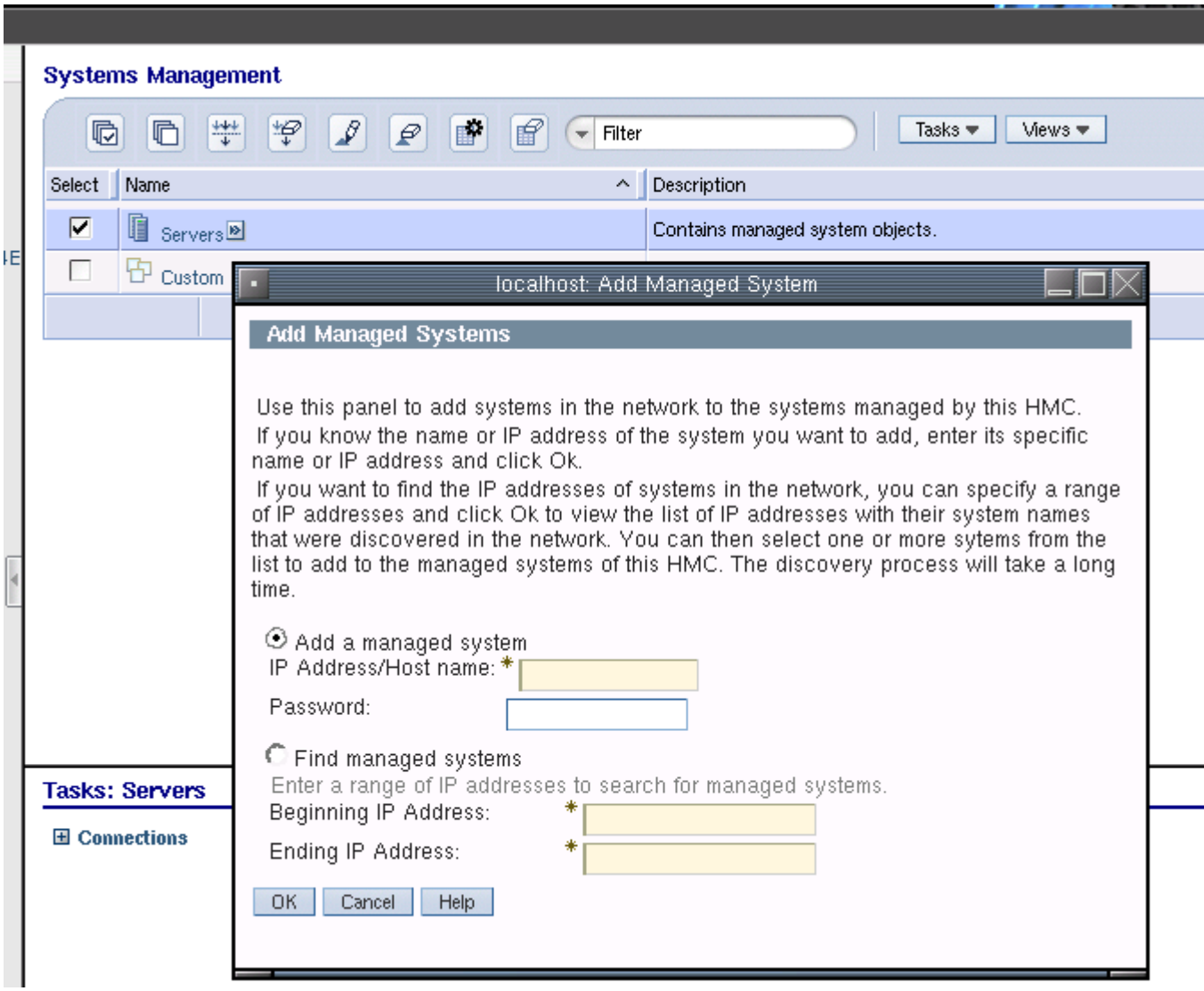
查看标红的端口有没有启动侦听。

49.Power 服务器硬件监控

可通过 IBM HMC 硬件管理控制台系统实现对 Power 系列服务器的基本信息读取和状态监控，当状态发生异常时产生告警。

1. 确认现场使用的 HMC 版本为 7 或以上版本
2. 添加服务器：

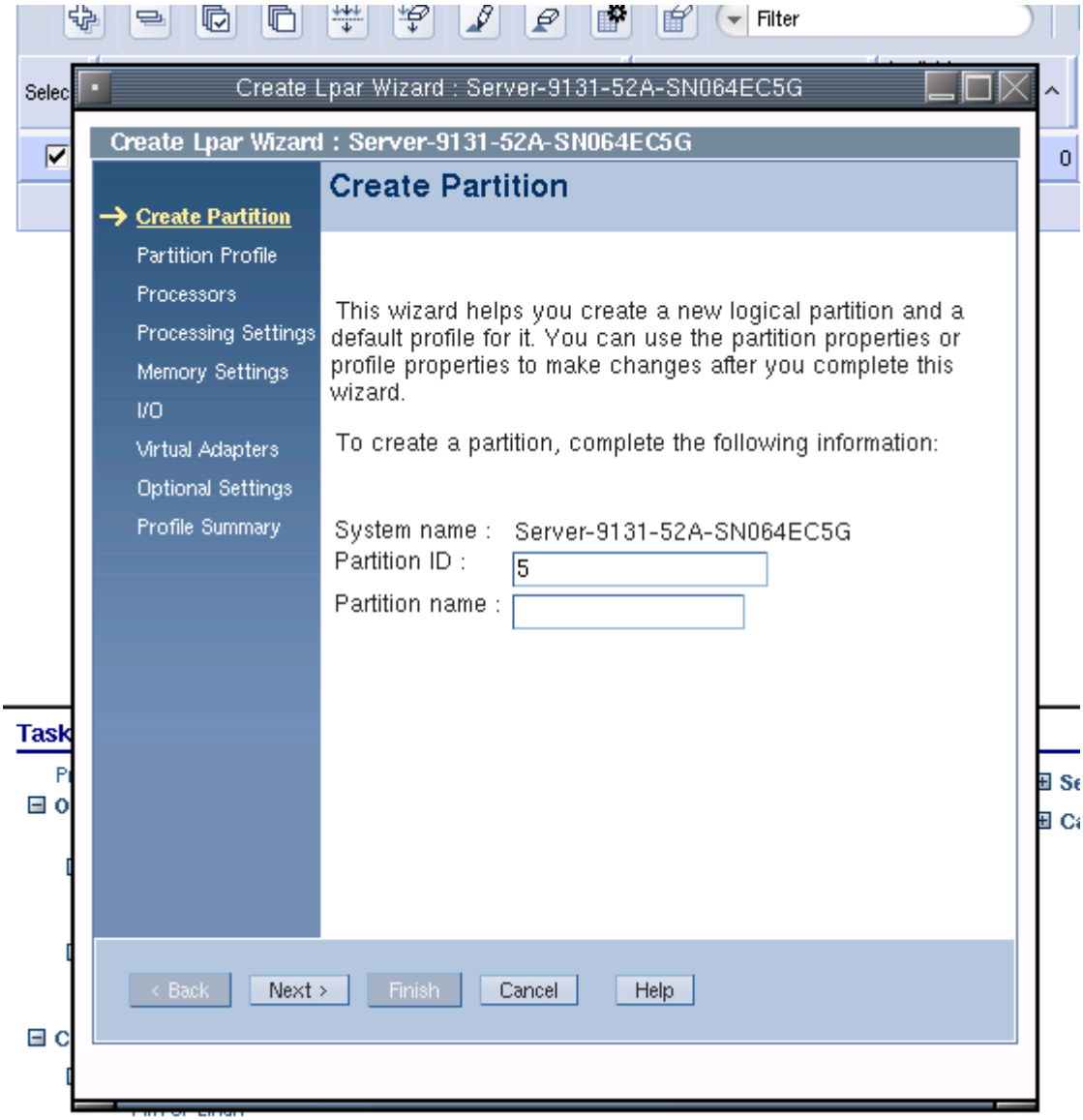
将 IBM Power 服务器添加到 HMC 中，如下图所示：



有两种添加方式：一种是直接添加某个服务器，需要填写 IP 地址和密码，这种方式可以添加不存在的服务器，而状态就是不可用了；另一种是通过扫描一个网段，扫描到的服务器都是真实存在的，然后添加的时候也需要填写密码。

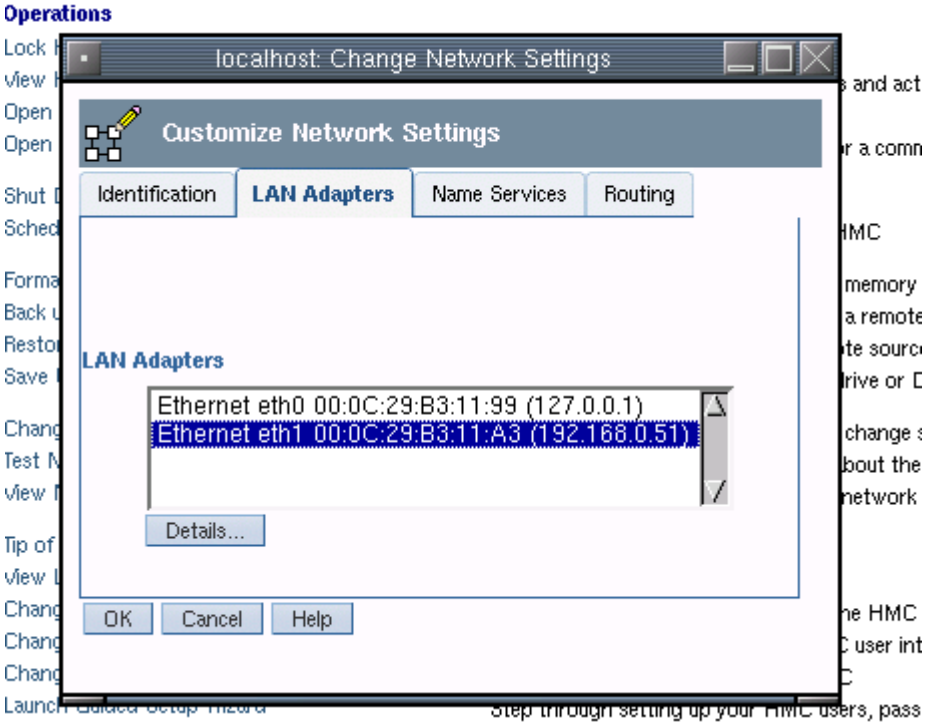
3. 添加逻辑分区

在某个服务器上添加逻辑分区，如下图所示：



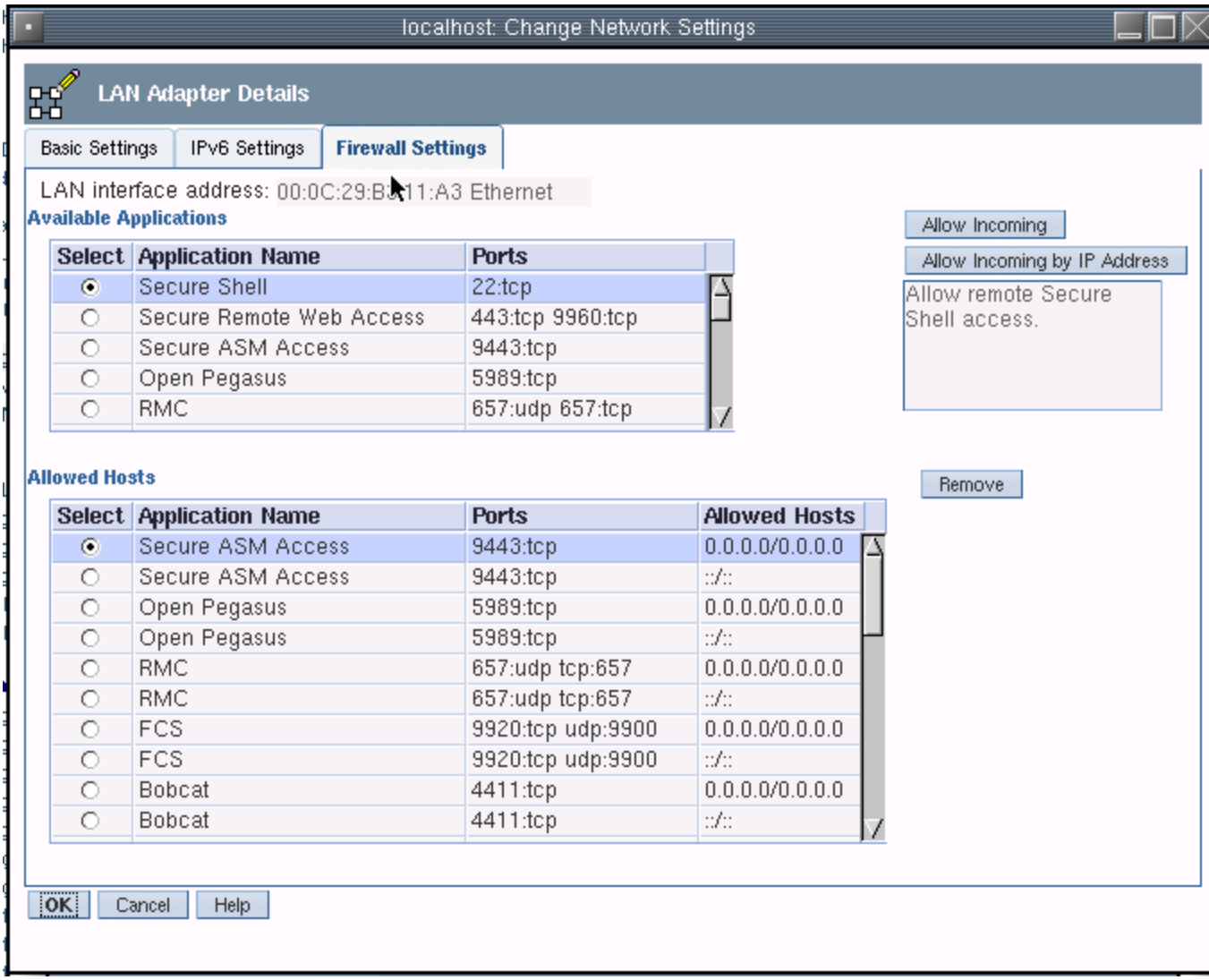
创建一个逻辑分区需要设定概要文件，分配处理器、内存、IO 资源，以及共享模式等等。

4. 通过网络设置设置一个对外的 IP，以便通过 ssh 进行连接：



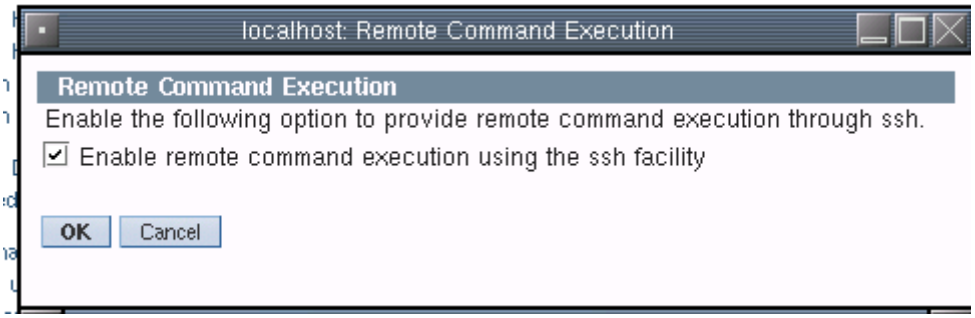
我这里设置的是 192.168.0.51，要设置这个 IP，首先需要在创建虚拟机的时候多创建一块网卡。

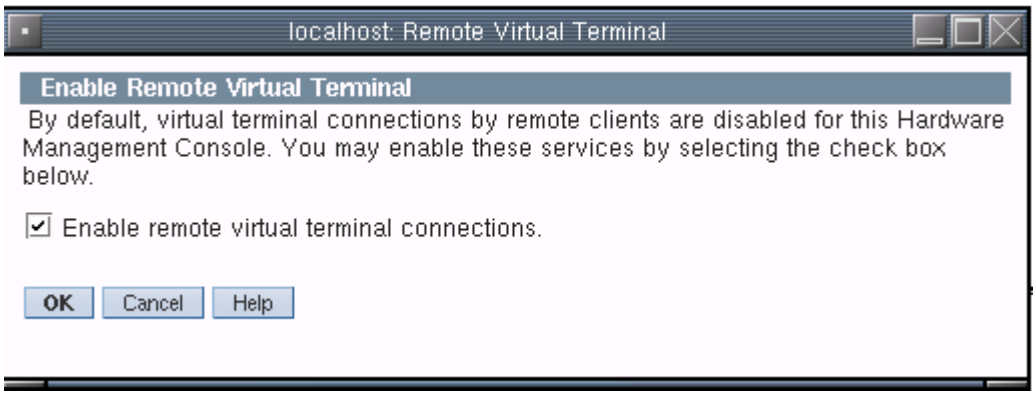
5. 开放防火墙，点击上图”Details”按钮，如下所示：



选择“Filewall Settings”选项卡，选中“Secure Shell”，点击右上角的“Allow Incoming”，表示允许所有 IP 访问此设备的 TCP:22 端口。

6. 允许远程访问，如下所示：





将远程命令执行和远程虚拟终端设为启用。

7. 通过 putty 以 SSH 的方式登录 HMC，HMC 的缺省用户名密码是“hscroot/abc123”。登录成功说明可以通过添加资源的方式进行添加。

50.HP EVA 磁盘阵列

1. 支持 HP EVA4400/6400 磁盘阵列，其它型号不保证完全兼容，可能会引起部分数据读取不全等问题

2. 下载 hp command view，下载地址：

https://h20392.www2.hp.com/portal/swdepot/displayProductsList.do?category=SWSDED

需按提示注册账号，登录后才能下载，下载的版本要根据 HP-EVA 的固件版本来选择：

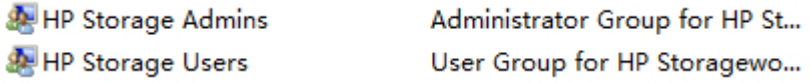
2.0 HP P6000 Command View Software interoperability support

This table lists the controller software and layered applications that are supported with HP P6000 Command View.
– HP P6000 Command View 9.4 includes HP P6000 Command View 9.4 for server-based management and array-based management, HP Command View EVAPerf 9.4, SMI-S EVA 9.4, and SSSU 9.4.
– HP P6000 Command View 10.0 includes HP P6000 Command View 10.0 for server-based management and array-based management, HP P6000 Performance Data Collector 10.0, HP P6000 Performance Advisor 10.0, HP SMI-S EVA 10.0, and SSSU 10.0.
– HP P6000 Command View Software Suite 10.1 includes HP P6000 Command view 10.1 for server-based management and array-based management, HP P6000 Performance Data Collector 10.1, HP P6000 Performance Advisor 10.1, HP SMI-S EVA 10.1, SSSU 10.1, HP P6000 SmartStart 4.1 and HP Management Integration Framework 1.5.
– HP P6000 Command View Software Suite 10.2 includes HP P6000 Command View 10.2 for server-based management and array-based management, HP P6000 Performance Data Collector 10.2, HP P6000 Performance Advisor 10.2, HP SMI-S EVA 10.2, SSSU 10.2, HP P6000 SmartStart 4.2, EVA to 3PAR Online Import 10.2 and HP Management Integration Framework 1.6.
– HP P6000 Command View Software Suite 10.3 includes HP P6000 Command View 10.3 for server-based management and array-based management, HP P6000 Performance Data Collector 10.3, HP P6000 Performance Advisor 10.3, HP SMI-S EVA 10.3, SSSU 10.3, HP P6000 SmartStart 4.3, HP EVA to 3PAR StoreServ Online Import 10.3 and HP Management Integration Framework 1.7.

	9.4[2] & 9.4.1[2]	10.0[2]	10.1[2,6]	10.2[2,8] & 10.2.1[2,8]	10.3
Controller software					
VCS 3.110/4.100[3,6A]	.[3]				
XCS 6.1xx[6A]	.[4]	.[4]	.[4]	.[4]	.
XCS 6.200, 6.220[6A]	.	.	.	.	.
XCS 6.240, 6.250	.	.	.	.	.
XCS 09501x00[6A]	.	.	.	.	.
XCS 0952x000[6A]	.	.	.	.	.
XCS 0953x000[6A]	.	.	.	.	.
XCS 10001000	.	.	.	.	.
XCS 11001100			.	.	.
XCS 11200000					.

注：版本不对应可能会导致部分数据取不到

2. 安装 hp command view，按提示安装即可，安装完以后会新建两个组，把用户加到对应的组里就行，如下图：



3. 添加 hp 磁盘阵列，hp command view 安装完以后可以自动识别连接的 hp 磁盘阵列
4. 连接测试，可用 CIM Browser 进行连接，url 为：http://commandViewIp:5988/root/eva
5. 上述步骤完成后，进入 IM 系统，按照常规添加被监控资源的步骤进行添加即可

51.拓扑链路发现的前置条件

设备与设备之间的拓扑链路发现功能，依赖于设备支持相关的网络协议、正确实现相关的 SNMP MIB、网管软件厂商本身的拓扑发现算法，网络设备本身需支持的规格为：

- 完整实现 RFC1213 MIB-II
- 完整实现 Bridge MIB
- 支持 STP/RSTP/MSTP 协议
- 支持 LLDP 协议（优选）
- 支持 CDP 协议（可选）
- 支持 NDP 协议（可选）
- 厂商可提供私有的链路发现协议（可选）

52.告警北向接口

告警北向接口的作用是与任意第三方系统集成，将 APEX IT 综合管理系统作为各种告警的集中处理平台，支持 HTTP 方式接收第三方系统产生的告警后通过短信、邮件方式通知管理员，提供事后查询、图表分析功能。

HTTP 请求方式：POST

URL：
http://xxx.xxx.xxx.xxx/oceanserver/ws/v1/alarmservice/newalarm/

请求参数：

参数名称	必填	类型	备注
access_token	false	string	集成第三方系统时不需要传入 access_token 字段
apiKey	true	string	申请得到的 API Key，当集成第三方系统的告警时必须传入，该 Key 需要在 APEX 系统中生成后告知第三方系统。
ipAddress	true	string	告警源的 IP 地址
resourceName	true	string	告警源的名称
alarmName	true	string	告警的名称
severity	true	int	1 表示紧急告警 2 表示重要告警 3 表示次要告警 4 表示一般性的警告信息
cause	true	string	告警的详细描述，最大不得超过 512 个字符
raiseTime	true	string	告警的产生时间，格式为 yyyy-MM-dd

			HH:mm:ss，比如 2012-11-01 18:51:45

返回结果：

接收第三方系统告警后，是否处理的结果，接收第三方系统发送过来的告警时需要进行校验，JSON 示例：

```
{
    "result": true,
    "error": ""
}
```

或者

```
{
    "result": false,
    "error": "保存失败，ApiKey非法."
}
```

或者

```
{
    "result": false,
    "error": "请求参数错误，XXX字段格式错误."
}
```

53. 告警转发

告警转发的意思是当 APEX IT 综合管理系统监测到 IT 资源故障时，出于系统集成的需要，能够通过某种协议将告警转发给第三方系统，目前支持的转发协议为 SNMP TRAP v1，下表详细描述了 TRAP 的定义。

OID	数据类型	说明
.1.3.6.1.4.1.8989.1.1	octet string	告警的类型
.1.3.6.1.4.1.8989.1.2	Ipaddress	告警故障源的 IP 地址
.1.3.6.1.4.1.8989.1.3	octet string	告警的详情描述
.1.3.6.1.4.1.8989.1.4	octet string	告警的产生时间
.1.3.6.1.4.1.8989.1.5	Integer32	告警的级别 1：紧急告警 2：重要告警 3：次要告警 4：警告告警
.1.3.6.1.4.1.8989.1.6	octet string	告警源设备的位置
.1.3.6.1.4.1.8989.1.7	octet string	告警的 id，是告警记录的数据库主键