

**云南省地方税务局**

**IT资源管控平台**

**设备部署指南**

上海天玑科技股份有限公司

二零一四年十一月

**IT资源管控平台**

**设备部署指南**

目录

[1 概述 4](#_Toc404177314)

[1.1 目的 4](#_Toc404177315)

[1.2 范围 4](#_Toc404177316)

[1.3 术语 4](#_Toc404177317)

[1.4 参考文档 5](#_Toc404177318)

[2 监控前准备 6](#_Toc404177319)

[2.1 网络条件 6](#_Toc404177320)

[2.2 设备条件 6](#_Toc404177321)

[2.3 实施规划建议 7](#_Toc404177322)

[3 主机系统 8](#_Toc404177323)

[3.1 Linux 8](#_Toc404177324)

[3.2 HP-UX 8](#_Toc404177325)

[3.3 AIX 8](#_Toc404177326)

[3.4 Windows 9](#_Toc404177327)

[3.4.1 WMI 9](#_Toc404177328)

[3.4.2 SNMP 16](#_Toc404177329)

[4 网络设备 18](#_Toc404177330)

[5 数据库系统 19](#_Toc404177331)

[5.1 Oracle/Oracle RAC 19](#_Toc404177332)

[5.2 Sybase 20](#_Toc404177333)

[5.3 MS SqlServer 23](#_Toc404177334)

[6 应用中间件 26](#_Toc404177335)

[6.1 Weblogic/Weblogic Cluster 26](#_Toc404177336)

[6.2 WebSphere MQ 26](#_Toc404177337)

[6.2.1 Unix/Linux 26](#_Toc404177338)

[6.2.2 Windows 26](#_Toc404177339)

[6.3 IIS 26](#_Toc404177340)

[6.4 Apache 26](#_Toc404177341)

[7 存储设备 28](#_Toc404177342)

[7.1 磁盘阵列 28](#_Toc404177343)

[7.2 光纤交换机 28](#_Toc404177344)

# 概述

## 目的

本文档用于说明云南省地方税务局IT资源管控平台（以下简称本系统）对被监控系统（主机、数据库、网络设备、中间件等）的访问权限要求以及网络通信要求。本文档不包含“机房监控”部分。

## 范围

本文档的读者范围包括本系统管理人员以及本产品的开发人员和实施人员。

## 术语

* **HTTP**

超文本传送协议 (HTTP-Hypertext transfer protocol) 定义了浏览器（即万维网客户进程）怎样向万维网服务器请求万维网文档，以及服务器怎样把文档传送给浏览器。从层次的角度看，HTTP是面向（transaction-oriented)[应用层协议](http://baike.baidu.com/view/10562159.htm)，它是万维网上能够可靠地交换文件（包括文本、声音、图像等各种多媒体文件）的重要基础。

* **JDBC**

JDBC（Java Data Base Connectivity,java[数据库](http://baike.baidu.com/view/1088.htm)连接）是一种用于执行SQL语句的Java API，可以为多种关系数据库提供统一访问，它由一组用[Java语言](http://baike.baidu.com/view/229611.htm)编写的类和接口组成。JDBC提供了一种基准，据此可以构建更高级的工具和接口，使[数据库](http://baike.baidu.com/view/1088.htm)开发人员能够编写数据库[应用程序](http://baike.baidu.com/view/330120.htm)。

* **JMX**

JMX（Java Management Extensions，即Java管理扩展）是一个为[应用程序](http://baike.baidu.com/view/330120.htm)、[设备](http://baike.baidu.com/view/209665.htm)、系统等植入管理功能的框架。JMX可以跨越一系列异构[操作系统](http://baike.baidu.com/view/880.htm)平台、[系统体系结构](http://baike.baidu.com/view/3928625.htm)和[网络传输协议](http://baike.baidu.com/view/16807.htm)，灵活的开发无缝集成的系统、网络和服务管理应用。

* **SMI-s**

SMI-S协议由美国存储网络工业协会(SNIA)所提出，存储管理建议规范(Storage Management Initiative Specification)简称为SMI-s

SMI-S主旨是把存储网络的管理对象，以及用来管理对象的工具统一起来，最终让所有的存储网络部件都可以利用本地的SMI-S接口加以部署。如此可以使所有的部件都采用一种通用的接口，管理功能的实现就更方便，成本也更低，系统更稳定。此外，稳定的管理接口有助于文件系统和数据库管理程序等应用系统直接管理网络存储资源。

* **SNMP**

简单网络管理协议（SNMP），由一组网络管理的标准组成，包含一个[应用层](http://baike.baidu.com/view/239619.htm)协议（application layer protocol）、[数据库模型](http://baike.baidu.com/view/598718.htm)（database schema）和一组资源对象。该协议能够支持[网络管理系统](http://baike.baidu.com/view/2523209.htm)，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。该协议是互联网工程工作小组（IETF，Internet Engineering Task Force）定义的internet协议簇的一部分。

* **SSH**

[SSH](http://baike.baidu.com/subview/16184/5909253.htm) 为 [Secure Shell](http://baike.baidu.com/view/2118359.htm) 的缩写，由 IETF 的[网络](http://baike.baidu.com/view/3487.htm)工作小组（Network Working Group）所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠，专为[远程登录](http://baike.baidu.com/view/59099.htm)会话和其他网络服务提供安全性的协议。

* **WMI**

WMI（Windows Management Instrumentation,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。

* **WSMQ API**

WebSphere Message Queue 是IBM提供的消息中间件，可以通过其提供的管理API来监控MQ。

## 参考文档

* 《WMI技术指南》--
* 《System Administration Guide》 –Sybase
* MSDN SQL Server – Microsoft
* 《Programming WebLogic Management Services with JMX》--Oracle
* IBM Knowledgecenter – WebSphere MQ 7.1 – IBM

# 监控前准备

## 网络条件

本系统所有的监控手段均基于TCP/IP协议，因此需要能够建立监控系统与被监控设备之间基于TCP/IP协议的网络连接，这种连接可以被限制到被监控设备的某个端口。不管基于何种监控技术，被监控设备提供的端口都有可能不同于默认端口。

* **HTTP**

用于监控用户的HTTP服务器，HTTP服务器的常用端口有80,8080。

* **JDBC**

JDBC是JAVA程序访问数据库的常用方法，不同的数据库采用不同的默认端口。

* **JMX**

JMX主要用于监控Weblogic对象,其端口是Weblogic的Admin Server端口。

* **SMI-s**

SMI-s主要用于监控存储设备,SMI-s本身基于http协议,其默认端口是5988(http)，5989(https)。

* **SNMP**

SNMP是网络管理的最重要协议之一,主要用于监控网络设备设备。SNMP使用UDP协议，其默认端口是161。

* **SSH**

SSH协议主要用于监控Unix/Linux主机，SSH协议默认端口是22。

* **WMI**

WMI协议用于监控Windows主机,默认需要打开135、139、445端口。

* **WSMQ API**

WebSphere MQ的默认端口是1414。

## 设备条件

1. 被监控设备需要提供本系统采用的特定协议

这些协议在被管系统上一般以“服务”的方式提供，如ssh,snmp,wmi等，但并不是所有服务都是默认安装或开启的，这些设备在被监控之前需要安装并启动这些“服务”。

1. 被管设备需要授权本系统通过特定的协议访问其资源

一些被管设备对访问授权提供了非常精细的控制能力，不同的授权方案会限制本系统对被管设备的监控范围，甚至导致不能监控。同样，过分的授权也会导致潜在的安全隐患。

建议用户根据本文档所提要求进行授权。

## 实施规划建议

对于主机设备、数据库设备、中间件等被管设备，实施监控需要通过用户名、密码验证的方式访问被管设备，为便于管理，建议针对本系统创建统一的用户名和密码。

# 主机系统

## Linux

Linux系统需要提供ssh服务以及通过ssh访问系统的账号。

需要创建一个属于adm,sys组的用户

|  |
| --- |
| useradd –u 275 –g sys –G adm,sys itzygk |

【说明】

* 此用户被授权通过SSH访问系统，要求用户的网络系统允许探针所在的机器可以通过ssh协议访问采集对象，默认端口为22。
* 如果用户不能被授予sys组的权限，那么逻辑卷管理(LVM)的相关信息将无法获取。
* 如果用户不能被授予adm组的权限，那么单个CPU的利用率信息将无法获取。

## HP-UX

HP-UX系统需要提供ssh服务以及通过ssh访问系统的账号。

需要创建一个属于users组的用户

|  |
| --- |
| useradd –u 275 –d /home/itzygk itzygk |

【说明】

* sar命令需要对所有用户都有执行权限

|  |
| --- |
| $ ls -l /usr/sbin/sar  -r-xr-xr-x 1 bin bin 123300 Oct 29 2008 /usr/sbin/sar  $chmod 555 /usr/sbin/sar |

## AIX

AIX系统需要提供ssh服务以及通过ssh访问系统的账号。

需要创建一个属于adm,staff组的用户

|  |
| --- |
| mkuser id=275 home=/home/itzygk shell=/usr/bin/ksh –g “adm,staff” itzygk |

**或者**

|  |
| --- |
| [/]id itzygk  [/]useradd –g adm,staff -u 275 itzygk  [/]passwd itzygk  第一个命令检查用户itzygk是不是存在  第二个命令增加一个用户，  第三个命令用于设置密码  **然后**  [/] ssh 172.40.1.102 -l itzygk  --会提示你修改密码，  然后再配置到监控系统中 |

【说明】

* 需要赋予itzygk用户执行swap命令的权限 (否则需要将用户加入sys组)

|  |
| --- |
| #]cd /home/itzygk  #]cp /usr/bin/swap .  #]chmod 755 swap  #]chown itzygk:staff swap  执行以下命令，显示swap信息  #]./swap -l |

* 如果不赋予用户adm组的权限，将不能采集单个CPU的信息

## Windows

对Windows系统的监控可以提供两种方式，WMI和SNMP,建议使用WMI方式，在不具备WMI采集条件的情况下，可以使用SNMP采集方式。

WMI方式需要操作系统用户账号，SNMP方式则不需要。相应的SNMP方式可以采集的信息少于WMI方式。

### WMI

#### 增加用户

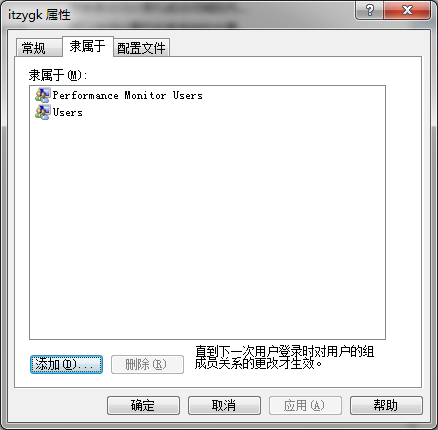
1. 属于Performance Monitor Users组的用户，密码不能为空。

**该用户不需要远程登录桌面的权限。**

计算机管理（本地）-系统工具-本地用户和组-用户

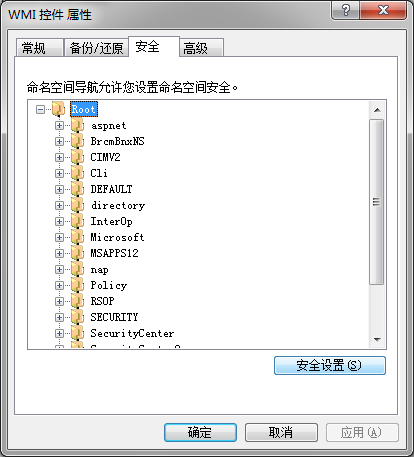
右键-新用户





#### WMI控件属性

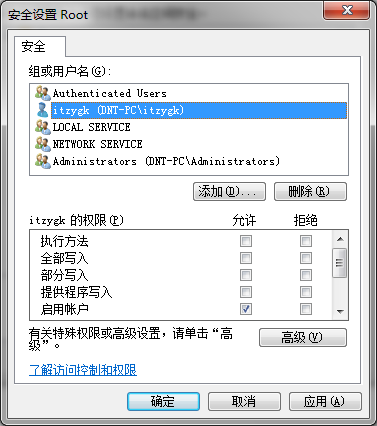
计算机管理（本地）- 服务和应用程序 – WMI控件 – 安全



选择【安全设置】，点击【添加】



点击【高级】，选择需要添加的用户并确认。



选择用户，并设置以下权限为允许，并点击【应用】

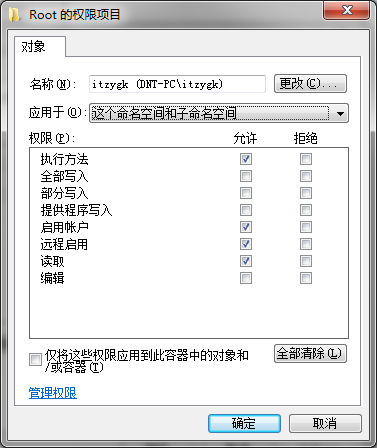
* + 执行方法
  + 启用账户
  + 远程启用
  + 读取

点击【高级】



点击【编辑】

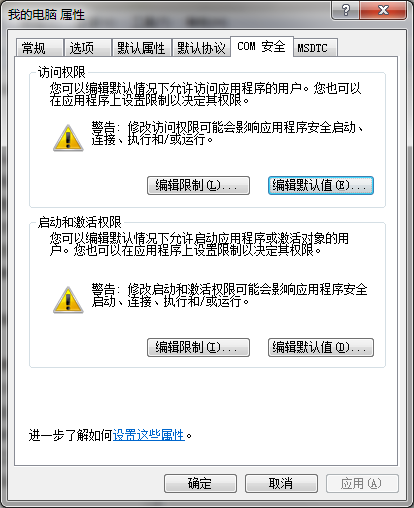
应用于选择“这个命名空间和子空间”，点击【确定】



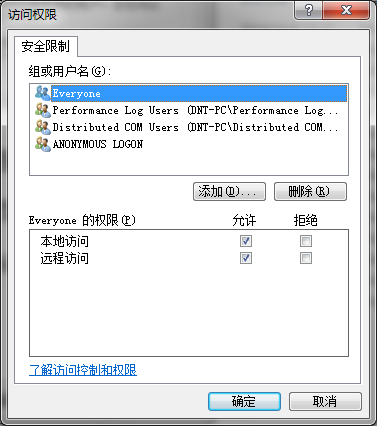
点击若干个【确定】之后关闭WMI控件属性

#### DCOM授权

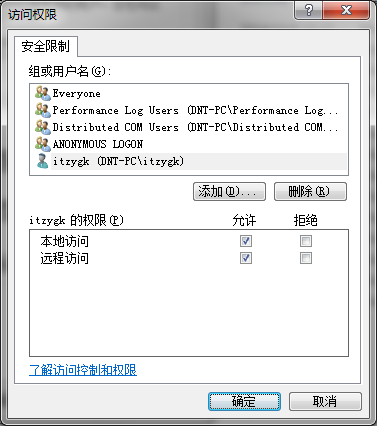
在命令行运行dcomcnfg命令，选择 组件服务-计算机-我的电脑，右键选择【属性】，选择COM安全



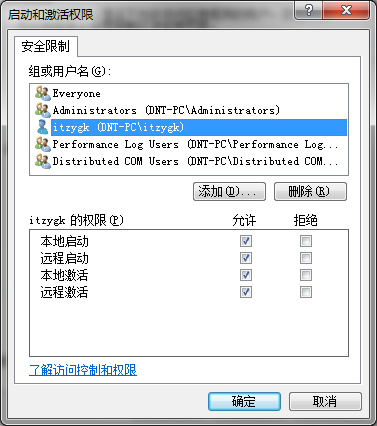
访问权限【编辑限制】



点击【添加】，添加选择的用户，并赋予远程访问的权限。



启动和激活权限【编辑限制】



赋予以下权限

* + 本地启动
  + 远程启动
  + 本地激活
  + 远程激活

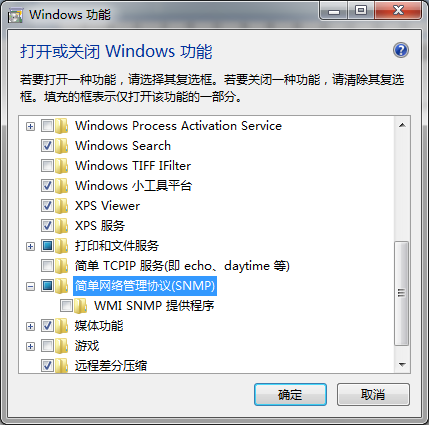
选择【确定】

### SNMP

#### 启用SNMP服务

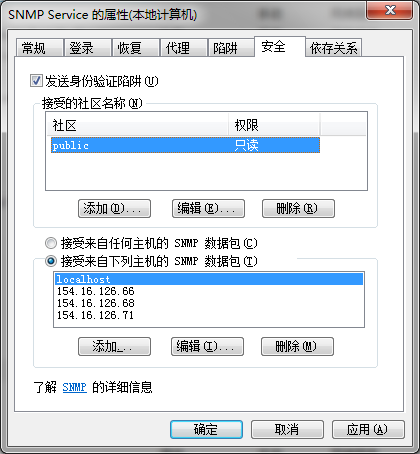
控制面板-程序和功能-打开或关闭Windows功能,

选择【简单网络管理协议(SNMP)】，点击确定

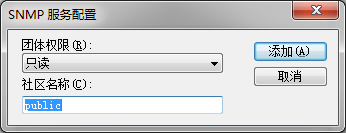


#### SNMP Service 属性

计算机管理-服务和应用程序-选择服务-Snmp Service，点击右键，选择【属性】



添加社区：



也可以【接收来自下列主机的SNMP数据包】，然后【添加】相应的IP地址

# 网络设备

本系统通过SNMP协议访问所有类型的被管网络设备。

* 被管设备需要启动SNMP服务，并授权本系统的采集引擎所在机器访问被管设备。
* 需要提供访问SNMP服务的Community名称。
* 网络管理员如果修改了默认的内容视图(限制一些MIB内容是否可见)，可能会导致一些必须的数据无法采集。

# 数据库系统

## Oracle/Oracle RAC

以下命令需要具有SYSDBA权限的用户执行

|  |
| --- |
| SQL>create user itzygk identified by itzygk default tablespace users ;  SQL>grant connect to itzygk ;  SQL>grant select on v\_$database to itzygk;  SQL>grant select on v\_$instance to itzygk;  SQL>grant select on v\_$osstat to itzygk;  SQL>grant select on v\_$pgastat to itzygk;  SQL>grant select on v\_$sgastat to itzygk;  SQL>grant select on v\_$sysstat to itzygk ;  SQL>grant select on v\_$parameter to itzygk ;  SQL>grant select on gv\_$session to itzygk ;  SQL>grant select on gv\_$log to itzygk ;  SQL>grant select on v\_$lock to itzygk;  SQL>grant select on v\_$session to itzygk;  SQL>grant select on v\_$session\_wait to itzygk;  SQL>grant select on sys.dba\_objects to itzygk;  SQL>grant select on v\_$locked\_object to itzygk;  SQL>grant select on v\_$sqltext to itzygk;  SQL>grant select on v\_$sqlstats to itzygk;  SQL>grant select on v\_$logfile to itzygk;  SQL>grant select on v\_$log to itzygk;  SQL>grant select on dba\_data\_files to itzygk;  SQL>grant select on dba\_tablespaces to itzygk;  SQL>grant select on dba\_free\_space to itzygk ; |

## Sybase

1. **创建用户**

用户名itzygk,密码ynds2014,允许在所有数据库登录.







1. **赋予itzygk对master..syslisteners表的select权限**

|  |
| --- |
| [root@YFDSS bin]# ./isql -U sa -P dnt123 -S YFDSS  1> use master  2>go  1>grant select on syslisteners to itzygk  2>go  Authorization updated.  (return status = 0)  1> |

1. **赋予itzygk对各数据库的sysquerymetrics表的select权限**

以下数据库上运行的SQL不再监控范围内：

**'model','tempdb','sybsystemprocs','sybsystemdb'**

因此无需赋予权限

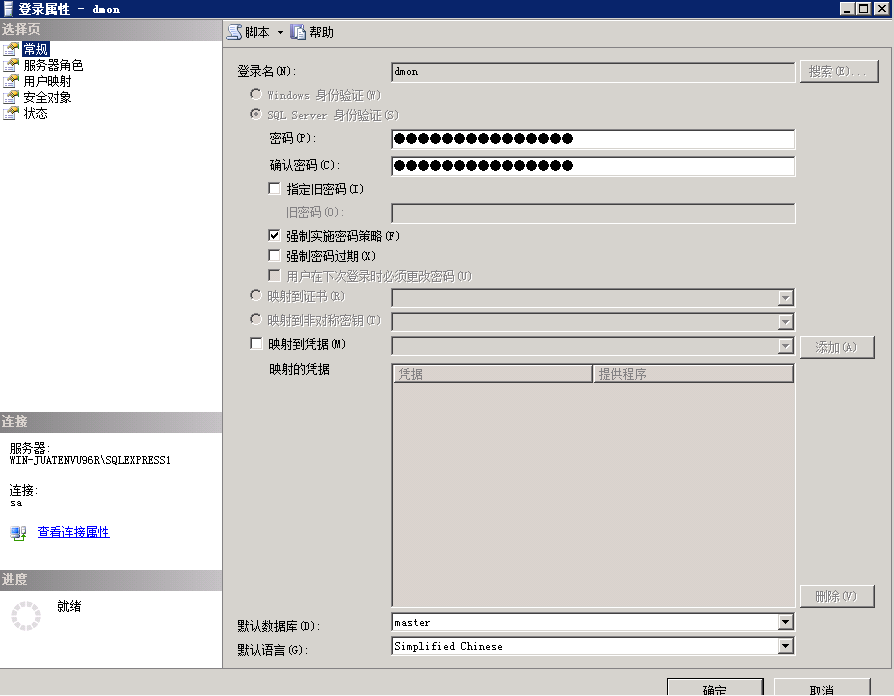
|  |
| --- |
| [root@YFDSS bin]# ./isql -U sa -P dnt123 -S YFDSS  1> use master  2>go  1>grant select on sysquerymetricsto itzygk  2>go  Authorization updated.  (return status = 0)  1>use <dbname>  2>go  1> grant select on sysquerymetricsto itzygk  2>go |

1. **权限清单**

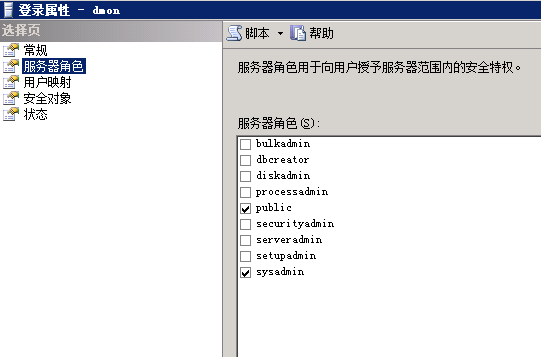
|  |  |  |
| --- | --- | --- |
| 权限 | 数据库 | 数据库表 |
| SELECT |  | @@SERVERNAME |
| SELECT |  | @@VERSION |
| SELECT |  | @@boottime |
| SELECT |  | @@CPU\_BUSY |
| SELECT |  | @@IDLE |
| SELECT | master | sysdatabases |
| SELECT | master | sysusages |
| SELECT | master | sysdevices |
| SELECT | master | syslocks |
| SELECT | master | spt\_values |
| SELECT | master | sysprocesses |
| SELECT | master | syslogins |
| SELECT | master | sysengines |
| SELECT | master | sysconfigures |
| SELECT | master | syscurconfigs |
| SELECT | each | syssegments |
| SELECT | each | sysquerymetrics |
| SELECT | each |  |
| 执行 | sp\_helpsegment |  |

## MS SqlServer

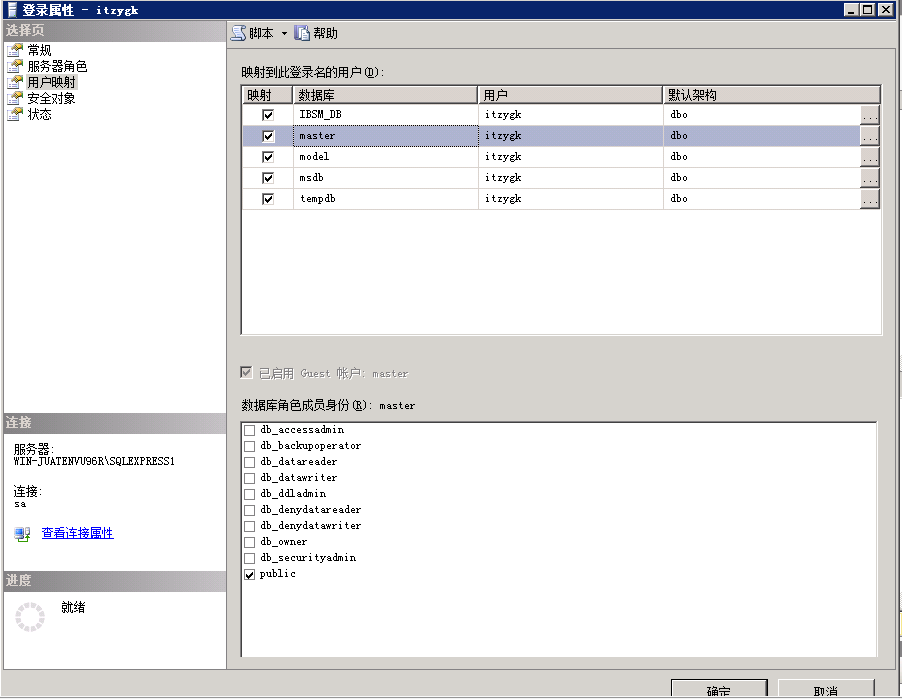
1. **创建用户**



1. **授予用户public 和 sysadmin 角色**



1. **将此用户映射到所有数据库**



1. **权限清单**

|  |  |  |
| --- | --- | --- |
| 权限 | 数据库 | 数据库表 |
| SELECT |  | @@SERVERNAME |
| SELECT |  | @@SERVICENAME |
| SELECT |  | @@VERSION |
| SELECT |  | @@CPU\_BUSY |
| SELECT |  | @@IDLE |
| SELECT | master | sys.dm\_os\_performance\_counters |
| SELECT | master | sys.dm\_exec\_query\_stats |
| SELECT | master | sys.dm\_exec\_sql\_text |
| SELECT | master | dm\_exec\_sessions |
| SELECT | master | dm\_exec\_connections |
| SELECT | master | sysprocesses |
| SELECT | master | master\_files |
| SELECT | master | sysaltfiles |
| SELECT | master | syslockinfo |
| SELECT | master | sysdatabases |
| 执行 | sp\_server\_info |  |

# 应用中间件

## Weblogic/Weblogic Cluster

1. 在安全领域中允许**使用授权提供程序保护 JMX 访问**
2. 在安全领域中增加一个监控专用的用户，此用户属于”monitors”组即可。

## WebSphere MQ

WebSphere MQ可以安装在从IBM大型机(Z/OS)到笔记本电脑的广泛平台中，本文档仅描述MQ安装在Linux,Unix(HP-UX,AIX),以及Windows平台上的情况。

### Unix/Linux

用户名mqm(用户mqm是系统安装时指定的)，默认没有密码。或者属于mqm组的用户。

### Windows

需要创建一个属于mqm组（IBM Websphere MQ管理组）和Users组的用户。

## IIS

IIS通过WMIC方式访问，且仅支持安装在服务器版本中的IIS，要求同[3.4.1](#_WMI)。

## Apache

需要apache httpd 开放服务器状态监控

**For Linux/Unix**

修改httpd.conf中的以下配置（去掉注释）。

|  |
| --- |
| <location /c-server-status>  SetHandler server-status  Order Deny,Allow  Deny from nothing  Allow from all  </location>  ExtendedStatus On |

**For Windows**

修改httpd.conf的以下内容，去掉LoadModule status\_module之前的注释(#),并增加

ExtendedStatus和<Location>…</Location> 部分

|  |
| --- |
| LoadModule status\_module modules/mod\_status.so  <location /c-server-status>  SetHandler server-status  Order Deny,Allow  Deny from nothing  Allow from all  </location>  ExtendedStatus On |

Location之后的页面名称可以自己定义，应避免使用默认的server-status。

# 存储设备

## 磁盘阵列

如果设备没有内置SMI-s Provider,则：

* 1. 安装SMI-s Provider,需要提供
* 控制器IP地址,端口（默认）,管理员的用户名、密码
* 记录SMI-s Provider提供的阵列序列号
  1. 在SMI-s Provider中配置用户名、密码，用于访问SMI-s Provider

如果设备有内置SMI-s Provider,则：

1. 提供访问SMI-S Provider的IP地址,端口,用户名、密码

【说明】

SMI-s Provider的默认端口是5988(http),5989(https)，一般采用5989,可以输入

https://<IP>:5989/console 来检查是否有内置SMI-s Provider。

这里的IP可以是控制器IP(如IBM Storwize)，也可以是应用的IP(如HP EVA CommandView的IP)。

## 光纤交换机

通过SNMP协议访问，其要求同网络设备。