|  |
| --- |
| **XySoft Group** |
| **Tigase管理员文档** |
| v 0.1 |
|  |
| **XySoft Group** |
| **2018/4/19** |

密级：合作企业可见

|  |
| --- |
| 用于服务器部署、设置、优化、扩展、运维指南。 |

目录

[1.特性 4](#_Toc512003059)

[2.安装XMPP核心服务 5](#_Toc512003060)

[2.1 Windows环境下通过JAR安装（Dev环境较适合） 5](#_Toc512003061)

[2.2 Linux环境下安装（生产环境较适合） 9](#_Toc512003062)

[2.3 安装Web管理后台 10](#_Toc512003063)

[2.3.1 打开配置文件etc\init. properties 10](#_Toc512003064)

[2.3.2 增加HTTP API组件 10](#_Toc512003065)

[2.4 配置Message Archiving组件 12](#_Toc512003066)

[2.5 配置MUC组件 13](#_Toc512003067)

[2.6 配置HTTP API组件 16](#_Toc512003068)

[2.7 配置Socks 5组件 16](#_Toc512003069)

[2.8 配置AMP组件 16](#_Toc512003070)

[2.9 配置Load Balancing组件 16](#_Toc512003071)

[2.10配置Server Monitoring组件 16](#_Toc512003072)

[3 端口 17](#_Toc512003073)

[3.1 端口 17](#_Toc512003074)

[3.2 Iptable 设置开启端口 17](#_Toc512003075)

[4 系统配置 18](#_Toc512003076)

[4.1 Init.properties 18](#_Toc512003077)

[4.2 Tagase.conf 18](#_Toc512003078)

[4.3 数据存储配置 18](#_Toc512003079)

[4.4 JVM优化配置 18](#_Toc512003080)

[4.5 Session管理 18](#_Toc512003081)

[5安全设置 19](#_Toc512003082)

[5.1 服务器证书 19](#_Toc512003083)

[5.1.1 在PEM文件中创建和加载服务器证书 19](#_Toc512003084)

[5.1.2 安装LetsEncrypt（ free trusted CA）证书 19](#_Toc512003085)

[5.2 客户端证书 19](#_Toc512003086)

[5.3 自定义身份验证 19](#_Toc512003087)

[5.3.1 自带认证 19](#_Toc512003088)

[5.3.2 自定义认证连接器 19](#_Toc512003089)

[5.3.3 LDAP身份验证连接 19](#_Toc512003090)

[5.3.4 SASL外部扩展 19](#_Toc512003091)

[5.4包过滤安全 20](#_Toc512003092)

[5.4.1 基于域的包过滤 20](#_Toc512003093)

[5.5访问控制列表 20](#_Toc512003094)

[6数据库管理 20](#_Toc512003095)

[6.1 推荐数据库版本 20](#_Toc512003096)

[6.2 数据库准备 20](#_Toc512003097)

[6.3 哈希用户密码 20](#_Toc512003098)

[6.4 多数据库分库分表 20](#_Toc512003099)

[6.5 导入User数据 20](#_Toc512003100)

[6.6 导入已有数据 21](#_Toc512003101)

[6.7 更新数据库 21](#_Toc512003102)

[7高级配置 21](#_Toc512003103)

[7.1 日志指南 21](#_Toc512003104)

[7.2 服务器调试 21](#_Toc512003105)

[7.3 运行环境检查 21](#_Toc512003106)

[7.3.1 BOSH 21](#_Toc512003107)

[7.3.2 Web Socket 21](#_Toc512003108)

[7.4 Scripting 扩展支持 22](#_Toc512003109)

[7.5 服务器命令行操作 22](#_Toc512003110)

[7.6 集群配置 22](#_Toc512003111)

# 1.特性

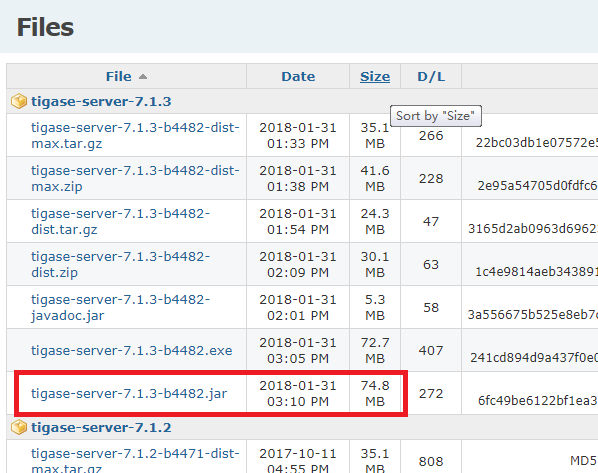
* **服务器健壮可靠**
  + 处理许多并发请求/连接，并且可以可靠地长时间运行。服务器被设计和实现以处理数百万个同时连接。
  + 项目的主要重点放在测试，使用专门的测试框架，所有服务器功能都只在通过严格的测试周期时才被发行。测试周期包括3个基本测试：
  + 功能测试-检查函数是否工作。
  + 性能测试-检查函数是否执行得足够好。
  + 稳定性测试-检查该函数在长期运行中是否运行良好。
  + 它必须在几百小时的服务器运行中处理数百个请求。
* **安全的通信平台。**
  + 安全的数据传输，SSL或TLS协议；
  + 安全的用户授权，DIGEST或者SASL用户授权架构支持；
  + 会话管理基于私有网络，使用DMZ管理连接客户端，DMZ使内部私有网络隔离于Internet；
* **灵活，可以应用于不同的场景。**
  + 对于大型企业或因特网门户服务器来说，通常负载非常重，必须支持成千上万的同时连接。对于这样的部署，我们需要较高级别的安全性，和较复杂的配置，比如集群。
  + 对于小型网络，关键因素是易于部署和维护。基于组件的体系结构提供了可选模块的能力，服务器可以很容易地应用在任何场景中。
  + 对于简单的安装，服务器生成一个配置文件，可以直接使用。
  + 对于复杂的部署，可以调整你的需要配置，并且灵活扩展到许多物理机器。
* **可扩展，充分利用XMPP协议的可扩展性。**
  + 可以很容易地添加新的功能。
  + 采用模块化结构。
  + 可以很容易地替换那些不符合你需求的组件，更好地满足你的需求。
  + 在服务器设计API中投入了大量的注意力，使得软件开发人员更容易创建扩展和实现新的特性。
* **易于安装和维护。**
  + 小公司只需要几个服务器来满足他们的需要，默认的配置可以立刻运行服务。
  + 允许动态配置，在运行过程中更改配置设置不需要重新启动服务器。
  + 还可以使用API接口和Web用户界面用于服务器监控。

# 2.安装XMPP核心服务

## 2.1 Windows环境下通过JAR安装（Dev环境较适合）

进入下载地址<https://tigase.tech/projects/tigase-server/files>

下载 **.jar文件**

****

用cmd运行

java -jar D:\0Tigase\tigase-server-7.1.3-b4482.jar

建议用java8 sdk

第12步的配置文本（你的和我的不同）：

--comp-class-1 = tigase.http.HttpMessageReceiver

http/setup/admin-credentials = admin:tigase

--admins = admin@WIN7-1803071731

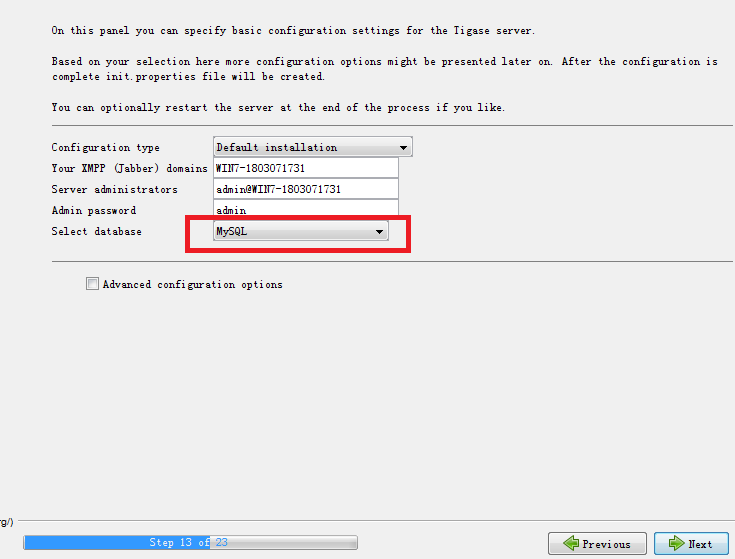
config-type = --gen-config-def

--virt-hosts = WIN7-1803071731

--debug = server

--comp-name-1 = http

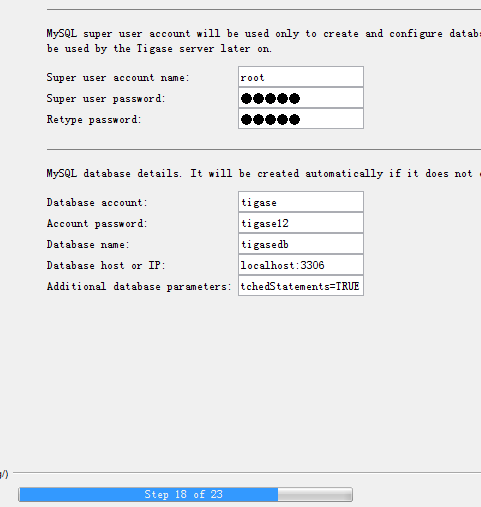
第13步：选MySQL



第18步

Additional MySQL参数：

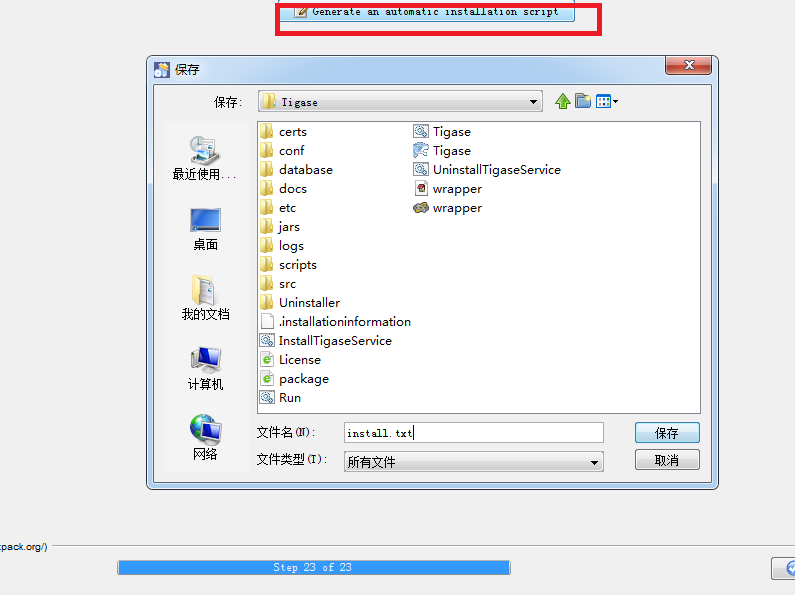
useUnicode=true&characterEncoding=utf8&**autoReconnect**=true&rewriteBatchedStatements=TRUE



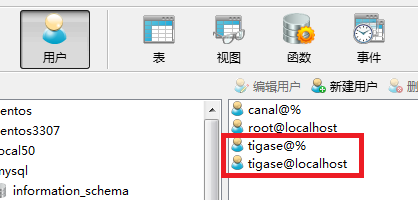
第19步会出现配置文件

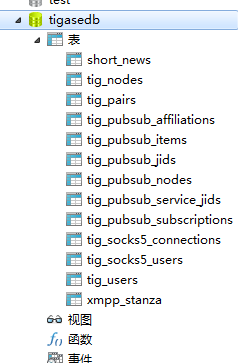


最后一步，可以选择是否建立自动化安装脚本，这个为日后的重装恢复做准备，脚本是一个XML文件（建议命名为install.xml），不做安装脚本也没问题。



看看数据库用户和表安装是否成功:





**运行  InstallTigaseService.bat，**把服务加入Windows服务

**运行Run.bat启动**

On a **Linux** system you may start the server using the **tigase** file found in the **scripts** sub-directory of Tigase server base directory. You will need to select the type of linux you have, debian, gentoo, mandirva, or redhat, and use the script located in the init.d folder. In the root server directory type the following command:

./scripts/{OS}/init.d/tigase start etc/tigase.conf

## 2.2 Linux环境下安装（生产环境较适合）

## 2.3 安装Web管理后台

### 2.3.1 打开配置文件etc\init. properties

Tigase的模块都是在配置文件init. properties里定义的，比如安装后的配置文件如下：

--virt-hosts = WIN7-1803071731

--user-db-uri = jdbc:mysql://localhost:3306/tigasedb?user=tigase&password=tigase12

--user-db = mysql

--admins = admin@WIN7-1803071731

config-type = --gen-config-def

--comp-name-4 = message-archive

--comp-name-3 = proxy

--comp-name-2 = pubsub

--comp-name-1 = muc

--comp-class-4 = tigase.archive.MessageArchiveComponent

--comp-class-3 = tigase.socks5.Socks5ProxyComponent

--comp-class-2 = tigase.pubsub.PubSubComponent

--comp-class-1 = tigase.muc.MUCComponent

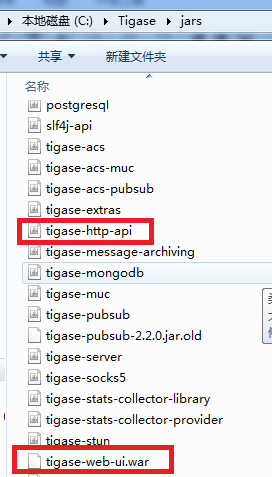
--cluster-mode = true

--sm-plugins = +message-archive-xep-0136

--debug = server

### 2.3.2 增加HTTP API组件

HTTP API组件在安装后已经添加进jars目录了，所以不需要独立下载



如果要增加HTTP API模块，需要增加两行：

--comp-name-5=http

--comp-class-5=tigase.http.HttpMessageReceiver

然后重启tigase服务，即可进入管理后台

<http://localhost:8080/ui/>



## 2.4 配置Message Archiving组件

在配置文件init. properties里进行类似定义：

--comp-name-4 = message-archive

--comp-class-4 = tigase.archive.MessageArchiveComponent

message-archive/archive-repo-uri=jdbc:mysql://127.0.0.1:3306/tigasedb?user=tigase&password=tigase12&useUnicode=true&characterEncoding=UTF-8

--sm-plugins = +message-archive-xep-0136

sess-man/plugins-conf/message-archive-xep-0136/component-jid=message-archive@win7-1803071731

sess-man/plugins-conf/message-archive-xep-0136/default-store-method=body

sess-man/plugins-conf/message-archive-xep-0136/required-store-method=body

sess-man/plugins-conf/message-archive-xep-0136/auto=true

保存群聊消息

sess-man/plugins-conf/message-archive-xep-0136/store-muc-messages=value

保存 <body/> or <subject/> 元素

sess-man/plugins-conf/unified-archive/msg-archive-paths[s]=/message/body,/message/subject

## 2.5 配置MUC组件

Init配置：

--comp-name-4 = muc

--comp-class-4 = tigase.muc.MUCComponent

可选配置：

* **room-log-directory** 日志路径

muc/room-log-directory=/var/log/muc/

* **message-filter-enabled** 禁用消息过滤:

muc/message-filter-enabled[B]=false

* **presence-filter-enabled** 禁用即席状态:

muc/presence-filter-enabled[B]=false

* **search-ghosts-every-minute**  每分钟pinging occupants

muc/search-ghosts-every-minute[B]=true

* **ghostbuster-enabled** To disable active searching of ghosts in MUC Rooms:

muc/ghostbuster-enabled[B]=false

* **muc-allow-chat-states** 允许传输消息状态chat-states in MUC messages:

muc/muc-allow-chat-states[B]=true

* **muc-lock-new-room** 关闭创建muc后的默认锁:

muc/muc-lock-new-room[B]=false

* **muc-multi-item-allowed** 不允许一个用户使用多个资源同时进入muc,比如不允许用户同时用安卓和ios进入，即用户名唯一:

muc/muc-multi-item-allowed[B]=false

#### History Providers Parameters

* **history-db** Database type. 可选derby, mysql, memory, pgsql, sqlserver, none.

muc/history-db=none

* **history-db-uri** URI for database

muc/history-db-uri=jdbc:mysql:/database/tigasedbmuc

#### Public log

* **muc-logger-class** 定制化MUC logger:

muc/muc-logger-class=com.example.CustomLogger

CustomLogger类必须实现接口 tigase.muc.logger.MucLogger.

模块定义

muc/modules/jabber:iq:version[S]=tigase.component.modules.impl.JabberVersionModule

muc/modules/owner[S]=tigase.muc.modules.RoomConfigurationModule

muc/modules/presences[S]=tigase.muc.modules.PresenceModuleImpl

muc/modules/groupchat[S]=tigase.muc.modules.GroupchatMessageModule

muc/modules/invitations[S]=tigase.muc.modules.MediatedInvitationModule

muc/modules/urn:xmpp:ping[S]=tigase.component.modules.impl.XmppPingModule

muc/modules/unique[S]=tigase.muc.modules.UniqueRoomNameModule

muc/modules/disco[S]=tigase.muc.modules.DiscoveryModule

muc/modules/iqforwarder[S]=tigase.muc.modules.IqStanzaForwarderModule

muc/modules/admin[S]=tigase.muc.modules.ModeratorModule

muc/modules/privatemessages[S]=tigase.muc.modules.PrivateMessageModule

muc/modules/commands[S]=tigase.component.modules.impl.AdHocCommandModule

Tigase MUC Options

* tigase#presence\_delivery\_logic - allows configuring logic determining which presence should be used by occupant in the room while using multiple-resource connections under one nickname, following options are available:
  + PREFERE\_PRIORITY
  + PREFERE\_LAST
* tigase#presence\_filtering - (boolean) when enabled broadcasts presence only to selected affiliation groups
* tigase#presence\_filtered\_affiliations - when enabled tigase#presence\_filtering is enabled one can select affiliation which should receive presences, following are possible to select from:
  + owner
  + admin
  + member
  + none
  + outcast
* muc#roomconfig\_maxusers - Allows configuring of maximum users of room.

Configuring default room configuration in init.properties

muc/default\_room\_config/<option>=<value>

for example:

muc/default\_room\_config/tigase#presence\_delivery\_logic=PREFERE\_LAST

## 2.6 配置HTTP API组件

## 2.7 配置Socks 5组件

## 2.8 配置AMP组件

## 2.9 配置Load Balancing组件

## 2.10配置Server Monitoring组件

## 3 端口

### 3.1 端口

* 3478 (TURN or STUN, plain socket, TCP and UDP)
* 5349 (TURN or STUN, over TLS, TCP and UDP)
* 5222 (default XMPP socket port)
* 5223 (legacy XMPP socket port)
* 5269 (default s2s port, i.e.: federation support)
* 5277 (component protocol port, e.g.: for external components)
* 5280 (default BOSH port)
* 5290 (default WebSocket port)
* 8080 (HTTP API component port)
* 9050 (JMX Monitoring)

### 3.2 Iptable 设置开启端口

iptables -A INPUT -p tcp -m tcp --dport 5222 -j ACCEPT

iptables -A INPUT -p tcp -m tcp --dport 5223 -j ACCEPT

iptables -A INPUT -p tcp -m tcp --dport 5269 -j ACCEPT

iptables -A INPUT -p tcp -m tcp --dport 5277 -j ACCEPT

iptables -A INPUT -p tcp -m tcp --dport 5280 -j ACCEPT

iptables -A INPUT -p tcp -m tcp --dport 5290 -j ACCEPT

iptables -A INPUT -p tcp -m tcp --dport 8080 -j ACCEPT

iptables -A INPUT -p tcp -m tcp --dport 9050 -j ACCEPT

# 4 系统配置

## 4.1 Init.properties

## 4.2 Tagase.conf

## 4.3 数据存储配置

## 4.4 JVM优化配置

## 4.5 Session管理

# 5安全设置

## 5.1 服务器证书

### 5.1.1 在PEM文件中创建和加载服务器证书

### 5.1.2 安装LetsEncrypt（ free trusted CA）证书

## 5.2 客户端证书

## 5.3 自定义身份验证

### 5.3.1 自带认证

### 5.3.2 自定义认证连接器

### 5.3.3 LDAP身份验证连接

### 5.3.4 SASL外部扩展

## 5.4包过滤安全

### 5.4.1 基于域的包过滤

## 5.5访问控制列表

# 6数据库管理

## 6.1 推荐数据库版本

## 6.2 数据库准备

## 6.3 哈希用户密码

## 6.4 多数据库分库分表

## 6.5 导入User数据

## 6.6 导入已有数据

## 6.7 更新数据库

# 7高级配置

## 7.1 日志指南

## 7.2 服务器调试

## 7.3 运行环境检查

### 7.3.1 BOSH

### 7.3.2 Web Socket

## 7.4 Scripting 扩展支持

## 7.5 服务器命令行操作

## 7.6 集群配置

End.